Root numbers of abelian varieties and their Galois representations

Bisatt, Matthew David

Awarding institution:
King's College London

Root numbers of abelian varieties and their Galois representations

by

Matthew David Bisatt

Thesis

Submitted to King's College, London

for the degree of

Doctor of Philosophy

Faculty of Natural and Mathematical Sciences

23rd July, 2018

KING'S College LONDON

Contents

Acknowledgements

First and foremost, I would like to extend my deepest gratitude to Vladimir Dokchitser for his generous help and guidance throughout this research, as well as his patience and insight into this work. I am also grateful to my family and non-mathematical friends for supporting me through this, despite understanding very little. Last, but by no means least, I wish to thank the staff and students at both the University of Warwick and the University of London for answering all my little questions as well as providing the stress relief needed at times.

Declaration

I hereby declare that the results presented within are original (excepting Chapter 2 and unless otherwise stated) and have not been previously submitted towards any other qualification. Moreover, all work is my own, excepting the chapter entitled "Compatibility of the Birch–Swinnerton-Dyer conjecture and Schur indices" which is submitted as joint work with V. Dokchitser with each author doing an equal share of the work.

A significant portion of the chapter "Frobenius elements in images of Galois representations" has been accepted for publication by *Journal of Number Theory* [Bis18].

Abstract

The Birch–Swinnerton-Dyer conjecture is one of the most famous open problems in modern number theory; this is reflected by its inclusion in the Clay Mathematics Institute million-dollar problems. The conjecture asserts that the rank of an abelian variety can be recovered from its L-function. In this thesis, we examine some of the consequences that are predicted by the Birch–Swinnerton-Dyer conjecture with the aid of Galois representations.

The first consequence is the parity conjecture: this states that the expected sign of the functional equation, known as the root number, should control the rank modulo 2; i.e. whether it is odd or even. We derive explicit formulae for the root number in terms of Jacobi symbols, as well as their generalisation to twisted root numbers. This is a very useful tool for numerically verifying the Birch–Swinnerton-Dyer conjecture and we give worked examples of computing the root number associated to the Jacobian of a hyperelliptic curve. As an application, we give sufficient criteria for an abelian variety such that *every* quadratic twist has infinitely many rational points, assuming the parity conjecture.

If one combines the Birch–Swinnerton-Dyer conjecture with a conjecture of Deligne–Gross, then one can obtain a generalised version concerning twisted L-functions. One can then use tools from representation theory to give predictions about: orders of vanishing of the twisted L-functions; the corank of the ℓ^∞-Selmer group; and the existence of certain extensions where high orders of vanishing of the (untwisted) L-function always occur, independently of the abelian variety.

Finally, we investigate the classical problem of distinguishing conjugacy classes of Frobenius elements in images of Galois representations. Using elliptic curves as the source of our Galois representations, we present two algorithms to distinguish between conjugacy classes of matrix groups in a small number of situations.

Chapter 1

Introduction

Think of a polynomial equation with rational coefficients. Does it have solutions over the rationals? If so, how many? Can you describe all of them? This is one of the earliest types of problems in mathematics, dating back to Diophantus of Alexandria. These questions arguably spawned the branch of mathematics we now refer to as number theory and still persist today.

Whilst the problem is still unsolved for arbitrary polynomials (and indeed never will be due to a negative answer to Hilbert's 10th problem), there are still large classes for which we can say something about. One of these is the class of elliptic curves and abelian varities, which have become somewhat ubiquitous in modern number theory. In the 1920s, Mordell and Weil proved that the set of rational points of an abelian variety is finitely generated as an abelian group. Due to the presence of the Tate–Shafarevich group, checking whether an arbitrary abelian variety has infinitely many points is still a difficult question.

After running some computations in the 1960s, Birch and Swinnerton-Dyer found an alternative approach: they predicted that the rank should be connected to the number of points of the reduction of abelian variety over finite fields, information that we now package into its L-function. This is now known as the Birch–Swinnerton-Dyer conjecture and has reached such prominence that it was chosen to be one of seven million-dollar problems by the Clay Mathematics Institute.

The parity conjecture may be considered as the "modulo 2" version of the Birch–Swinnerton-Dyer conjecture. The main advantage though is that it is independent of the L-function which is in general not known to be defined at the critical point; in its place, one uses the global root number $W(A/\mathcal{K})$ of an abelian variety $A/\mathcal{K}$ over a

global field. Since the root number is conjecturally equal to the sign of the functional equation, it should control the parity of the order of vanishing of the L-function. The parity conjecture hence predicts that

$$W(A/\mathcal{K}) = (-1)^{\mathrm{rk}\, A/\mathcal{K}}.$$

In particular, if the parity conjecture is true, then a negative root number would imply that $A/\mathcal{K}$ has odd rank and hence infinitely many rational points, providing an answer to the classical question.

We begin in Chapter 3 with an investigation into root numbers and are able to give a complete description of the local root number as a product of Jacobi symbols, building on work of Rohrlich [Roh96]; the global root number is then simply the product over all places of local root numbers. Their simplicity provides an efficient tool for checking for infinitely many points; this is faster than the standard descent methods one uses to compute the rank.

Aside from the application of root numbers to a numerical verification of the Birch–Swinnerton-Dyer conjecture, the complete formulae for root numbers have played a vital role in the current proof of the parity conjecture for elliptic curves (assuming finiteness of the Tate–Shafarevich group) [DD11, Theorem 1.2] and to distribution results in families of elliptic curves [Hel04] and density results on elliptic surfaces [BDD16, Des16, VA11]. Our theorem below will enable further research into these questions in higher dimensions.

Theorem 1.0.1 (=Theorem 3.3.5)**.** *Let A/K be an abelian variety defined over a non-Archimedean local field of residue cardinality q, which has tame, potentially good reduction. Let m_e denote the multiplicity of eigenvalues of order e on the image of a generator of tame inertia (counted as a multiple of the Euler φ-function for $e \geqslant 3$; for their proper definition see §3.1.1). Then the local root number is*

$$W(A/K) = \prod_{e \in \mathbb{N}} W_{q,e}^{m_e},$$

where for an integer $k > 0$ and rational odd prime l:

$$W_{q,e} = \begin{cases} \left(\frac{q}{l}\right) & \text{if } e = l^k; \\ \left(\frac{-1}{q}\right) & \text{if } e = 2l^k \quad \text{and } l \equiv 3 \bmod 4 \qquad \text{or } e = 2; \\ \left(\frac{-2}{q}\right) & \text{if } e = 4; \\ \left(\frac{2}{q}\right) & \text{if } e = 2^k \quad \text{for } k \geqslant 3; \\ 1 & \text{else.} \end{cases}$$

This work follows a recent pattern of extending explicit arithmetic of elliptic curves to abelian varieties. Other such work includes that of Booker, Sijsling, Sutherland, Voight and Yasaki [BSS$^+$16] who have computed various invariants of genus two hyperelliptic curves as part of the LMFDB collaboration [Col17]; van Bommel's algorithms [vB17] to numerically verify the full Birch–Swinnerton-Dyer conjecture for Jacobians of hyperelliptic curves; and the upcoming paper of Dokchitser, Dokchitser, Maistret and Morgan [DDMM] who study the arithmetic of hyperelliptic curves.

Indeed, by using the results of [DDMM], we can go one step further and extract the relevant data from the defining polynomial of a hyperelliptic curve; these will be the source of our examples. Their results also enables us to completely recover all the root numbers computed in a recent paper of Brumer, Kramer and Sabitova [BKS18].

In Chapter 4, we study twisted root numbers for self-dual Artin representations; these analogously allow us to determine the parity of the order of vanishing of the corresponding twisted L-function. One can show that, according to a generalisation of the Birch–Swinnerton-Dyer conjecture to Artin twists, certain types of twists should always give an even order of vanishing, independently of the choice of abelian variety. This implies that the twisted root number is positive; a claim proved by Sabitova [Sab07] under some assumptions. We build on Sabitova's results with work from the previous chapter to give a description of the twisted root number in both the local and global setting. As an application of all our theory, we derive criteria for an abelian variety to have a root number which is invariant under quadratic twists. Moreover, we compute examples over $\mathbb{Q}$ (given in Appendix A) which are predicted by the parity conjecture to obtain additional rational points of infinite order over every quadratic extension. This is equivalent to stating that every quadratic twist has infinitely many rational points; a scenario that does not occur for elliptic curves over $\mathbb{Q}$.

Criterion A. Let A/K be an abelian variety over a non-Archimedean local field with

residue cardinality q. Suppose that A/K has potentially good and tame reduction.

Let $W_g = \prod_{2\nmid e} W_{q,e}^{m_e} \prod_{e=4 \text{ or } 2||e} W_{q,e/2}^{m_e}$.

Then A/K satisfies Criterion A if $W_g = 1$.

Theorem 1.0.2 (=Lemma 4.4.4 and Theorem 4.4.5)**.** *Let $A/\mathcal{K}$ be an abelian variety over a global field. Then the global root number of* every *quadratic twist of $A/\mathcal{K}$ is equal if both of the following criteria are satisfied:*

i. $\dim A$ *is even or $\mathcal{K}$ has no real places;*

ii. for every finite place v, $A/\mathcal{K}_v$ satisfies Criterion A.

Part of our motivation for studying twisted root numbers in Chapter 4 was due to the pecularity that certain twists should always give an even order of vanishing of the twisted L-function. This is however a special case of a wider phenomenon; we extend these ideas in Chapter 5 to construct for every prime p, an Artin twist such that the order of vanishing of the twisted L-function is always a multiple of p. As an example, we obtain the following theorem; this is joint work with V. Dokchitser and applies more generally to abelian varieties over number fields.

Theorem 1.0.3 (=Theorem 5.2.1)**.** *Let $E/\mathbb{Q}$ be an elliptic curve and let p, q be odd primes. Let τ be an irreducible faithful Artin representation of a Galois extension $\mathcal{F}/\mathbb{Q}$ with* $\mathrm{Gal}(\mathcal{F}/\mathbb{Q}) \cong C_q \rtimes C_{p^n}$ *non-abelian and with $p^n \nmid q-1$.*
(i) If the Birch–Swinnerton-Dyer conjecture for Artin twists (Conjecture 2.5.11) holds, then

$$\mathrm{ord}_{s=1}\, L(E/\mathbb{Q}, \tau, s) \equiv 0 \mod p.$$

(ii) If the ℓ-primary part of the Tate–Shafarevich group $Ш(E/\mathcal{F})[\ell^\infty]$ is finite, then

$$\langle X_\ell(E/\mathcal{F}), \tau \rangle \equiv 0 \mod p,$$

where ℓ is any prime and $X_\ell(E/\mathcal{F})$ is the Pontryagin dual of the ℓ^∞-Selmer group of $E/\mathcal{F}$ tensored with $\mathbb{Q}_\ell$, viewed as a representation of $\mathrm{Gal}(\mathcal{F}/\mathbb{Q})$.

By observing a rationality structure of one Galois representation, we can infer properties of our chosen twist. In particular, by measuring how far away our twist is from being rational through the use of Schur indices, we are able to show the high order of vanishing of the corresponding twisted L-function. We then study the ramifications of such predictions, including an equivalent statement for a particular class of modular

forms, and use Artin formalism to present corresponding statements about untwisted L-functions.

Corollary 1.0.4 (=Corollary 5.2.6)**.** *Let $\mathcal{F}/\mathbb{Q}$ be a Galois extension with $\mathrm{Gal}(\mathcal{F}/\mathbb{Q}) \cong C_q \rtimes C_{p^n}$ non-abelian for p, q odd primes, where the image of C_{p^n} in $\mathrm{Aut}\, C_q$ has order p^r and $p^n \nmid q-1$. Suppose $E/\mathbb{Q}$ is an elliptic curve such that $L(E/\mathcal{K}, 1) \neq 0$ for all proper subfields $\mathcal{K} \subsetneq \mathcal{F}$. If the Birch–Swinnerton-Dyer conjecture for Artin twists (Conjecture 2.5.11) holds, then*

$$\mathrm{ord}_{s=1}\, L(E/\mathcal{F}, s) \;\equiv\; 0 \mod p^{n-r}(p-1)(q-1).$$

For our final foray into the realm of Galois representations, the underlying theme of this thesis, we consider a more classical problem in Chapter 6: determining conjugacy classes of Frobenius elements. Dokchitser–Dokchitser have previously studied this by viewing the Galois group as a permutation group [DD13]; we instead use the mod l Galois representation of an elliptic curve to consider the Galois group as a matrix group. The additional linear structure enables us to present an algorithm for two different cases:

- Distinguishing SL_n-conjugacy from GL_n-conjugacy;
- Distinguishing between the conjugacy classes of order 4 elements in the quaternion group $Q_8 \hookrightarrow \mathrm{GL}_2(\mathbb{F}_3)$.

The results we have in this case are as follows.

Theorem 1.0.5. *(=Theorem 6.2.2) Let $E/\mathcal{K}$ be an elliptic curve over a number field such that $\mathrm{Im}\, \rho_{E,l} = \mathrm{SL}_2$ and let $\mathfrak{p}$ be a prime of $\mathcal{K}$ of absolute norm q such that $\mathfrak{p} \nmid l\Delta_E$. Let $\sigma \in \mathrm{SL}_2$ be GL_2-conjugate to $\rho_{E,l}(\mathrm{Frob}_\mathfrak{p})$ and suppose that the GL_2-conjugacy class of σ splits in SL_2.*

Let $\tilde{E}$ be the reduced curve at $\mathfrak{p}$ and suppose that (Q_1, Q_2) is an ordered basis of $\tilde{E}[l]$ such that the action of the Frobenius automorphism $x \mapsto x^q$ acts as $\sigma \in \mathrm{SL}_2$ on $\tilde{E}[l]$ with respect to (Q_1, Q_2).

Then $\rho_{E,l}(\mathrm{Frob}_\mathfrak{p})$, written with respect to a global ordered basis (P_1, P_2), is SL_2-conjugate to σ if and only if

$$\langle P_1, P_2\rangle_l \mod \mathfrak{p} \equiv \langle Q_1, Q_2\rangle_l^{k^2} \text{ for some } k \in \mathbb{Z},$$

where $\langle\ ,\ \rangle_l$ denotes the Weil pairing.

Theorem 1.0.6 (see Theorem 6.3.10 for more detail)**.** *Let $E/\mathcal{K}$ be an elliptic curve over a number field $\mathcal{K}$ and suppose that $\operatorname{Im}\rho_{E,3} \cong Q_8$. Fix a basis of $E[3]$ and let $i, j, k \in \operatorname{Aut}(E[3])$ be matrices corresponding to pairwise non-conjugate order 4 elements of $\operatorname{Gal}(\mathcal{K}(E[3])/\mathcal{K})$ with respect to this basis. Let $\mathfrak{p}$ be a prime of $\mathcal{K}$ such that $\mathfrak{p} \nmid 3\Delta_E$ and $\rho_{E,3}(\operatorname{Frob}_\mathfrak{p})$ is $\mathrm{GL}_2(\mathbb{F}_3)$-conjugate to i.*

Then there exists functions $F_i, F_j, F_k \in \mathcal{K}(E)$ (to be constructed later; see Proposition 6.3.16 for their general form) and a function $G \in \frac{\mathcal{O}_\mathcal{K}}{\mathfrak{p}}(\tilde{E})$ (also constructed later; here $\tilde{E}$ is the reduction of E at $\mathfrak{p}$) such that if F_i, F_j, F_k are distinct modulo $\mathfrak{p}$, then

i. $\rho_{E,3}(\operatorname{Frob}_\mathfrak{p})$ *is* $\operatorname{Gal}(\mathcal{K}(E[3])/\mathcal{K})$*-conjugate to i if and only if $F_i \equiv G \mod \mathfrak{p}$;*

ii. $\rho_{E,3}(\operatorname{Frob}_\mathfrak{p})$ *is* $\operatorname{Gal}(\mathcal{K}(E[3])/\mathcal{K})$*-conjugate to j if and only if $F_j \equiv G \mod \mathfrak{p}$;*

iii. $\rho_{E,3}(\operatorname{Frob}_\mathfrak{p})$ *is* $\operatorname{Gal}(\mathcal{K}(E[3])/\mathcal{K})$*-conjugate to k if and only if $F_k \equiv G \mod \mathfrak{p}$.*

1.1 Notation

We introduce some common notation that we will use throughout the thesis, distinguishing between global fields and local fields for the reader's benefit. Any chapter-specific notation will be further introduced as needed.

General notation (All Chapters):

$\mathcal{K}, \overline{\mathcal{K}}$	global field with algebraic closure $\overline{\mathcal{K}}$,
$\mathfrak{p}$	prime of $\mathcal{K}$,
$\langle\, , \rangle$	standard inner product of characters (embedding into $\mathbb{C}$ if necessary),
ρ^*	dual of a representation ρ,
ζ_n	primitive n^{th} root of unity.

Local fields notation (Chapters 2, 3, 4):

$K, \overline{K}$	non-Archimedean local field with algebraic closure $\overline{K}$,
$\mathcal{O}_K, \pi_K$	ring of integers with uniformiser π_K,
$v : K^\times \twoheadrightarrow \mathbb{Z}$	normalised valuation of K
$p > 0$	residue characteristic of K,
q	cardinality of the residue field of K,
Frob	an arithmetic Frobenius element of K,
I, P	absolute inertia and wild inertia groups of K,
$\mathcal{W}(\overline{K}/K)$	$\cong I \rtimes \langle \mathrm{Frob} \rangle$ absolute Weil group of K,
ι	a topological generator of the tame inertia group $I/P \cong \prod_{\ell \neq p} \mathbb{Z}_\ell$.

Root numbers notation (Chapters 2, 3, 4):

A/K	an abelian variety,
ψ	a non-trivial additive character of K,
ρ_A	the associated Weil–Deligne representation of A/K,
τ_v	an Artin representation of $\mathrm{Gal}(\overline{K}/K)$,
$W(A/K, \psi)$	$= W(\rho_A, \psi)$ the local root number of A/K,
$W(A/K, \tau_v, \psi)$	$= W(\rho_A \otimes \tau_v, \psi)$ the local twisted root number of A/K by τ_v.

Chapter 2

Background

2.1 Representations of the Weil group

In general, one attaches root numbers to representations rather than to abelian varieties and in particular we will define them for representations of the Weil group. We shall briefly recall all the relevant theory about Weil groups that we shall need here. None of the theory presented here is original and the interested reader should consult [Roh94] or [Tat79] for more details.

Definition 2.1.1. *The Weil group $\mathcal{W}(\overline{K}/K)$ of K is defined (as an abstract group) to be such that the following diagram commutes and has exact rows.*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & I & \longrightarrow & \mathcal{W}(\overline{K}/K) & \longrightarrow & \mathbb{Z} & \longrightarrow & 1 \\ & & \| & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & I & \longrightarrow & \mathrm{Gal}(\overline{K}/K) & \longrightarrow & \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) & \longrightarrow & 1 \end{array}$$

More explicitly, $\mathcal{W}(\overline{K}/K) = \{\mathrm{Frob}^n\, i \,|\, n \in \mathbb{Z}, i \in I\} \cong I \rtimes \mathbb{Z}$.

Furthermore, the Weil group has the locally profinite topology: I has the profinite subgroup topology of $\mathrm{Gal}(\overline{K}/K)$ and one imposes the discrete topology on $\mathcal{W}(\overline{K}/K)/I \cong \mathbb{Z}$.

Lemma 2.1.2. *The tame quotient $\mathcal{W}(\overline{K}/K)/P$ is isomorphic to the semidirect product $\langle \iota \rangle \rtimes \langle \mathrm{Frob} \rangle$ with the action given by*

$$\mathrm{Frob}\, \iota\, \mathrm{Frob}^{-1} = \iota^q.$$

Proof. The semidirect claim is a routine verification; we shall only prove the action is as stated. Note that ι is completely described by its action on $\pi_K^{1/e}$ with $p \nmid e$. Let $\iota(\pi_K^{1/e}) = \zeta_e \pi_K^{1/e}$ and note that we have $\mathrm{Frob}(\zeta_e) = \zeta_e^q$ by definition of the Frobenius element. Then

$$\begin{aligned}
\mathrm{Frob}\,\iota\,\mathrm{Frob}^{-1}(\pi_K^{1/e}) &= \mathrm{Frob}\,\iota(\xi\pi_K^{1/e}) \qquad \text{for some } e^{\text{th}} \text{ root of unity } \xi, \\
&= \mathrm{Frob}(\xi\zeta_e\pi_K^{1/e}) \qquad \text{as } \iota \text{ acts trivially on } \xi, \\
&= \mathrm{Frob}(\zeta_e)\,\mathrm{Frob}(\xi\pi_K^{1/e}), \\
&= \zeta_e^q \pi_K^{1/e}, \\
&= \iota^q(\pi_K^{1/e}).
\end{aligned}$$

□

Definition 2.1.3. *A complex Weil representation is a continuous homomorphism*

$$\rho : \mathcal{W}(\overline{K}/K) \to \mathrm{GL}(V),$$

for some complex vector space V. We say ρ is:

- unramified *if $\rho(I)$ is trivial;*
- tamely ramified *if $\rho(P)$ is trivial.*

We shall now give an example of a representation of the Weil group, which we shall need later.

Example 2.1.4. *Let $\ell \neq p$ be prime. Then for any $\sigma \in \mathcal{W}(\overline{K}/K)$, $\sigma(\zeta_{\ell^k}) = \zeta_{\ell^k}^{a_k}$ for some a_k coprime to ℓ, independent of our choice of ζ_{ℓ^k}.*

We define the ℓ-adic cyclotomic character $\chi_{cyc} : \mathcal{W}(\overline{K}/K) \to \mathbb{Z}_\ell^\times$ as $\chi_{cyc}(\sigma) := \varprojlim_k a_k$ with respect to a system $\{\zeta_{\ell^k}\}_{k\geqslant 1}$. Note that since a_k is independent of our choice of ζ_{ℓ^k}, this limit is defined. To see this, let $b \in \mathbb{Z}$ be coprime to ℓ such that $\zeta_{\ell^k}^{b\ell} = \zeta_{\ell^{k-1}}$. Then

$$\sigma(\zeta_{\ell^k}^{b\ell}) = \zeta_{\ell^k}^{b\ell a_k} = \zeta_{\ell^{k-1}}^{a_k}.$$

However, $\sigma(\zeta_{\ell^{k-1}}) = \zeta_{\ell^{k-1}}^{a_{k-1}}$ by definition and hence $a_k \equiv a_{k-1} \bmod \ell^{k-1}$ so the sequence converges.

Let $\tau \in \mathcal{W}(\overline{K}/K)$ and let $\chi_{cyc}(\tau) = \varprojlim_k b_k$. Then for all integers $k > 0$, $(\tau\sigma)(\zeta_{\ell^k}) = \sigma(\zeta_{\ell^k}^{a_k}) = \zeta_{\ell^k}^{a_k b_k}$. Hence $\chi_{cyc}(\tau\sigma) = \varprojlim_k a_k b_k = \chi_{cyc}(\tau)\chi_{cyc}(\sigma)$ so χ_{cyc} is indeed a homomorphism.

If we choose an embedding $\mathbb{Q}_\ell \hookrightarrow \mathbb{C}$, then χ_{cyc} defines a one-dimensional Weil representation. Furthermore, χ_{cyc} is unramified and $\chi_{cyc}(\mathrm{Frob}) = q$.

Unfortunately, continuous Weil representations necessarily have finite image of inertia (whenever $\ell \neq p$) which is insufficient for our purposes. To encompass all types of representations we use, we introduce the notion of a Weil–Deligne representation.

Definition 2.1.5. *A complex Weil–Deligne representation $\boldsymbol{\rho}$ is a pair (ρ, N) where ρ is a complex Weil representation*

$$\rho : \mathcal{W}(\overline{K}/K) \to \mathrm{GL}(V),$$

and $N \in \mathrm{End}(V)$ is nilpotent such that

$$\rho(\mathrm{Frob}) \cdot N \cdot \rho(\mathrm{Frob})^{-1} = qN$$

for all choices of $\mathrm{Frob} \in \mathcal{W}(\overline{K}/K)$.

We say that a Weil–Deligne representation (ρ, N) is:

- Frobenius-semisimple *if ρ is semisimple;*
- semisimple *if $N = 0$ and ρ is semisimple.*

Remark 2.1.6. *Every Weil representation ρ can be considered as the Weil–Deligne representation $\boldsymbol{\rho} = (\rho, 0)$; we shall make such identifications when necessary [Roh94, §4].*

Now we shall define our prototypical example of a Weil–Deligne representation which is not a Weil representation.

Example 2.1.7. *Let $\ell \neq p$ be prime and fix $i \in I$. Then similarly to the ℓ-adic cyclotomic character example, we have for some integer t_k:*

$$i(\pi_K^{1/\ell^k}) = \zeta_{\ell^k}^{t_k} \pi_K^{1/\ell^k}.$$

We define the ℓ-adic tame character $t_\ell : I \to \mathbb{Z}_\ell$ to be such that $t_\ell(i) \equiv t_k \bmod \ell^k$ with respect to compatible systems $\{\pi_K^{1/\ell^k}\}_{k\geqslant 1}$ and $\{\zeta_{\ell^k}\}_{k\geqslant 1}$ (i.e. $\zeta_{\ell^{k+1}}^{\ell} = \zeta_{\ell^k}$ for all $k > 0$). This is independent of the compatible system of uniformisers since any two differ by a unit which is acted upon trivially by inertia. However, it is not independent of the system $\{\zeta_{\ell^k}\}_{k\geqslant 1}$, hence t_ℓ is not canonical, but the image of $t_\ell(i) \in \mathbb{Z}_\ell$ under two

different compatible systems will differ by an element of $\mathbb{Z}_\ell^\times$.

More abstractly, recall that we have a (non-canonical) isomorphism of the tame inertia group $I/P \cong \prod_{\ell \neq p} \mathbb{Z}_\ell$; the tame character is just a projection onto the corresponding factor.

Definition 2.1.8. *Let $\ell \neq p$ be prime. The special representation $\mathrm{sp}(2)$ is the two dimensional ℓ-adic representation of $\mathrm{Gal}(\overline{K}/K)$ given by*

$$\mathrm{Frob}^n i \mapsto \begin{pmatrix} 1 & t_\ell(i) \\ 0 & q^n \end{pmatrix}.$$

This is now independent of the choice of compatible system $\{\zeta_{\ell^k}\}_{k \geqslant 1}$ for t_ℓ as different choices give isomorphic representations. Indeed if t'_ℓ is the tame character with respect to a different system, then $t_\ell = a t'_\ell$ for some unit $a \in \mathbb{Z}_\ell^\times$ and conjugating the above matrix by $\left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right)$ proves the independence.

Proposition 2.1.9 (see §4 of [Roh94])**.** *Let $\rho_\ell : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_n(E_\ell)$ be a continuous ℓ-adic representation for some finite extension $E_\ell/\mathbb{Q}_\ell$, $\ell \neq p$.*

i. There is a unique nilpotent endomorphism $N_\ell \in M_n(E_\ell)$ such that

$$\rho_\ell(i) = \exp(t_\ell(i) N_\ell)$$

for i in some open subgroup of I;

ii. $N_\ell = 0$ if and only if ρ_ℓ is trivial on an open subgroup of I;

iii. Fix an embedding $E_\ell \hookrightarrow \mathbb{C}$. Define $\rho : \mathcal{W}(\overline{K}/K) \to \mathrm{GL}_n(E_\ell) \hookrightarrow \mathrm{GL}_n(\mathbb{C})$ by

$$\rho(\mathrm{Frob}^n i) = \rho_\ell(\mathrm{Frob}^n i) \exp(-t_\ell(i) N_\ell),$$

for all $n \in \mathbb{Z}, i \in I$. Let N be the image of N_ℓ in $M_n(\mathbb{C})$ under this embedding. Then $\boldsymbol{\rho} = (\rho, N)$ is a complex Weil–Deligne representation.

iv. The isomorphism class of $\boldsymbol{\rho}$ is independent of the choices of Frob and t_ℓ.

Example 2.1.10. *As an example, we shall construct the corresponding Weil–Deligne representation for $\mathrm{sp}(2)$. First note that this has infinite image of inertia so $N \neq 0$. If we let $N = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, then this is nilpotent with $N^2 = 0$. Using the power series for*

$\exp$ *we see that if* $i \in I$*, then*

$$\exp(t_\ell(i)N) = 1 + t_\ell(i)N = \begin{pmatrix} 1 & t_\ell(i) \\ 0 & 1 \end{pmatrix}.$$

This agrees with $\mathrm{sp}(2)$ *on* I *and hence* N *is the desired nilpotent endomorphism. To find our corresponding Weil representation, we compute that*

$$\begin{pmatrix} 1 & t_\ell(i) \\ 0 & q^n \end{pmatrix} \begin{pmatrix} 1 & -t_\ell(i) \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & q^n \end{pmatrix}.$$

Hence the Weil–Deligne representation associated to $\mathrm{sp}(2)$ *is* (ρ, N)*, where*

$$\rho(\mathrm{Frob}^n i) = \begin{pmatrix} 1 & 0 \\ 0 & q^n \end{pmatrix}, \ N = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Remark 2.1.11. *It is worth noting that* $\mathrm{sp}(2)$ *is a reducible but indecomposable representation. One can construct similar indecomposable representations in higher dimensions which are denoted* $\mathrm{sp}(n)$*, but we shall not need them.*

We briefly define the standard operations on Weil–Deligne representations. The equivalent operations for ℓ-adic representations commute with the construction of the associated Weil–Deligne representation [Roh94, §3].

Definition 2.1.12. *Let* $\boldsymbol{\rho}_1 = (\rho_1, N_1), \boldsymbol{\rho}_2 = (\rho_2, N_2)$ *be complex Weil–Deligne representations on vector spaces* V_1, V_2 *respectively. We define:*

i. the direct sum $\boldsymbol{\rho}_1 \oplus \boldsymbol{\rho}_2 = (\rho_1 \oplus \rho_2, N_1 \oplus N_2)$*;*

ii. the tensor product $\boldsymbol{\rho}_1 \otimes \boldsymbol{\rho}_2 = (\rho_1 \otimes \rho_2, N_1 \otimes 1_{V_2} + 1_{V_1} \otimes N_2)$*, where* 1_{V_j} *is the identity automorphism on* V_j*,* $j = 1, 2$*;*

iii. the dual representation $\boldsymbol{\rho}_\mathbf{1}^* = (\rho_1^*, N_1^*)$ *on the dual space* V_1^**, where*

$$(\rho_1^*(g)f)(v) = f(\rho_1(g)^{-1}v), \qquad (N_1^* f)(v) = -f(N_1 v),$$

for all $g \in \mathcal{W}(\overline{K}/K), f \in V_1^*, v \in V_1$*.*

Theorem 2.1.13 (Classification)**.** *Let* $\boldsymbol{\rho}$ *be an indecomposable, finite-dimensional, Frobenius-*

semisimple Weil–Deligne representation. Then

$$\rho \cong \theta \otimes \nu \otimes \mathrm{sp}(n),$$

for some irreducible Weil representation θ with finite image, unramified one dimensional Weil representation ν and integer $n \geqslant 1$. Moreover $\boldsymbol{\rho}$ is irreducible if and only if $n = 1$, where $\mathrm{sp}(1) := \mathbb{1}$ is the trivial representation.

Proof. See [Del73, Proposition 3.1.3]. □

2.2 ε-factors

Local root numbers are defined in terms of ε-factors; in this section we shall briefly state the important properties we use. For more detail, see for example [Tat79, pp.13,15] or [Roh94, p.144]. Whilst we will rarely ever deal with ε-factors directly, the majority of the properties we use for root numbers are derived from the ε-factor. Moreover, it is more apparent that ε-factors are dependent on some choices that our root numbers will not be so this will allow us to prove independence properly.

Let $\chi : K^\times \to \mathbb{C}^\times$ be a character. Using the Artin map, we can identify χ with a character of the Weil group $\mathcal{W}(\overline{K}/K)$. Let ψ be a non-trivial additive character of K and dx an additive Haar measure on K. Tate gives explicit formulae for computing $\varepsilon(\chi, \psi, dx) \in \mathbb{C}^\times$ and discusses the properties of ε-factors that allow one to uniquely extend the definition to arbitrary dimension.

Theorem 2.2.1. *[Tat79, p.15] Let χ be a one dimensional unramified complex representation of the Weil group over K. Then*

$$\varepsilon(\chi, \psi, dx) = \frac{\chi(\pi_K^{n(\psi)})}{||\pi_K^{n(\psi)}||} \int_{\mathcal{O}_K} dx,$$

where $n(\psi)$ is the conductor exponent of ψ, i.e. the largest n such that $\psi(\pi^{-n}\mathcal{O}_K) = 1$.

Let ρ, ρ' be two finite dimensional Weil representations of $\mathcal{W}(\overline{K}/K)$ and let ρ^* be the dual of ρ. Let $a(\rho)$ denote the Artin conductor exponent of ρ.

i. $\varepsilon(\rho \oplus \rho', \psi, dx) = \varepsilon(\rho, \psi, dx)\varepsilon(\rho', \psi, dx)$.

ii. Let K/H be a finite extension, ψ_H a non-trivial additive character of H and dx_H

an additive Haar measure on H. Suppose $\dim \rho = \dim \rho'$. Then

$$\frac{\varepsilon(\mathrm{Ind}_{K/H}\,\rho, \psi_H, dx)}{\varepsilon(\mathrm{Ind}_{K/H}\,\rho', \psi_H, dx)} = \frac{\varepsilon(\rho, \psi_H \circ \mathrm{Tr}_{K/H}, dx_H)}{\varepsilon(\rho', \psi_H \circ \mathrm{Tr}_{K/H}, dx_H)},$$

where $\mathrm{Tr}_{K/H}$ is the trace map and $\mathrm{Ind}_{K/H}$ is the induction map from $\mathcal{W}(\overline{K}/K)$ to $\mathcal{W}(\overline{K}/H)$.

iii. $\varepsilon(\rho \otimes \rho', \psi, dx) = \varepsilon(\rho, \psi, dx)^{\dim \rho'}((\det \rho')(\pi_K^{a(\rho)+n(\psi)\dim \rho}))$ *if ρ' is unramified.*

iv. $\varepsilon(\rho \oplus \rho^*, \psi, dx) = ((\det \rho)(-1))q^{a(\rho)+n(\psi)\dim(\rho)}$.

Remark 2.2.2. *Note that above we are associating the Weil representation $\det \rho$ with the corresponding representation on $K^\times$ via the Artin map and this is where the character should be computed on -1 and π_K; we shall leave such an identification implicit and switch between them freely.*

Remark 2.2.3. *One can also define ε-factors for a Weil–Deligne representation $\boldsymbol{\rho}$ by connecting it to the ε-factor of its semisimplification which may be viewed as a Weil representation. We will however use known results for our computations in this case so will not concern ourselves with this, but note that if $\boldsymbol{\rho} = (\rho, 0)$ is semisimple, then $\varepsilon(\boldsymbol{\rho}, \psi, dx) = \varepsilon(\rho, \psi, dx)$.*

Definition 2.2.4. *Let $\boldsymbol{\rho}$ be a Weil–Deligne representation of $\mathcal{W}(\overline{K}/K)$ and let ψ, dx be a non-trivial additive character and Haar measure of K. Then the local root number of $\boldsymbol{\rho}$ is*

$$W(\boldsymbol{\rho}, \psi, dx) = \frac{\varepsilon(\boldsymbol{\rho}, \psi, dx)}{|\varepsilon(\boldsymbol{\rho}, \psi, dx)|}.$$

Remark 2.2.5. *If $r > 0$ then $\varepsilon(\boldsymbol{\rho}, \psi, rdx) = r^{\dim \boldsymbol{\rho}}\varepsilon(\boldsymbol{\rho}, \psi, dx)$ (see [Tat79, p.15]). This shows the root number $W(\boldsymbol{\rho}, \psi, dx)$ is completely independent of the choice of Haar measure dx so we shall completely drop this part of the notation.*

Corollary 2.2.6. *(to Theorem 2.2.1) Let ρ be a finite dimensional Weil representation, ψ an additive character and dx a Haar measure. Then:*

i. $W(\rho \otimes \chi_{cyc}^k, \psi, dx) = W(\rho, \psi, dx)$ *for any $k \in \mathbb{R}$;*

ii. $W(\rho \oplus \rho^*, \psi, dx) = (\det \rho)(-1)$.

We now do an extended example to compute the root number of a particular Galois representation to give a flavour of how they are computed in practice.

Example 2.2.7. *Let* $G = \mathrm{Gal}(\mathbb{Q}_3(\zeta_5, \sqrt[5]{3})/\mathbb{Q}_3)$. *Then*

$$G = \langle \mathrm{Frob}, i | \, \mathrm{Frob}^4, i^5, \mathrm{Frob}\, i\, \mathrm{Frob}^{-1} = i^2 \rangle \cong C_5 \rtimes C_4.$$

The conjugacy classes of G *have representatives* $\mathrm{Id}, i, \mathrm{Frob}, \mathrm{Frob}^2, \mathrm{Frob}^3$*; its character table is below.*

G	Id	i	Frob	Frob^2	Frob^3
$\mathbb{1}_G$	1	1	1	1	1
sign	1	1	-1	1	-1
χ	1	1	ζ_4	-1	ζ_4^3
$\overline{\chi}$	1	1	ζ_4^3	-1	ζ_4
ρ	4	-1	0	0	0

We wish to compute the root number of the Weil representation ρ*. Let* $I = \langle i \rangle$ *be the inertia subgroup and let* ϕ *be any non-trivial one-dimensional representation of* I *and* $\mathbb{1}_I$ *the trivial representation on* I*. Then:*

$$\begin{aligned} \mathrm{Ind}_I^G \mathbb{1}_I &= \mathbb{1}_G \oplus \mathrm{sign} \oplus \chi \oplus \overline{\chi}, \\ \mathrm{Ind}_I^G \phi &= \rho. \end{aligned}$$

Let $K = \mathbb{Q}_3$ *and* $F = \mathbb{Q}_3(\zeta_5)$*, the subfield fixed by inertia. Let* dx_K, dx_F *be additive Haar measures on* K, F *respectively and let* ψ_K, ψ_F *be non-trivial additive characters of* K, F *such that* $\psi_F = \psi_K \circ \mathrm{Tr}_{F/K}$*.*

By Theorem 2.2.1ii, we have

$$\frac{\varepsilon(\rho, \psi_K, dx_K)}{\varepsilon(\mathbb{1}_G, \psi_K, dx_K)\varepsilon(\mathrm{sign}, \psi_K, dx_K)\varepsilon(\chi, \psi_K, dx_K)\varepsilon(\overline{\chi}, \psi_K, dx_K)} = \frac{\varepsilon(\phi, \psi_F, dx_F)}{\varepsilon(\mathbb{1}_I, \psi_F, dx_F)}.$$

This enables us to compute $\varepsilon(\rho)$ *by computing* ε*-factors of one-dimensional representations.*

Observe that each of the representations $\mathbb{1}_G, \mathrm{sign}, \chi, \overline{\chi}$ *is unramified so we can apply the definition directly to compute their* ε*-factors. To do this, we should choose a Haar measure and an additive character; we choose the normalised Haar measure so* $dx_K(\mathcal{O}_K) = 1$ *and any* ψ_K *with* $\ker \psi_K = \mathcal{O}_K$*, i.e.* $n(\psi_K) = 0$*. Our choices imply that* $\varepsilon(\eta, \psi_K, dx_K) = \eta(1) = 1$ *for all them and hence* $\varepsilon(\rho, \psi_K, dx_K) = \dfrac{\varepsilon(\phi, \psi_F, dx_F)}{\varepsilon(\mathbb{1}_I, \psi_F, dx_F)}$*. We could have instead used Theorem 2.2.1i and iv to compute* $\varepsilon(\chi, \psi_K, dx_K)\varepsilon(\overline{\chi}, \psi_K, dx_K)$*, noting that* $\chi(-1) = 1$ *as it is unramified.*

Since F/K is unramified, one can check (using the inverse different) that $n(\psi_F) = 0$ as well and hence choosing the Haar measure dx_F such that $dx_F(\mathcal{O}_F) = 1$, we similarly have $\varepsilon(\mathbb{1}_I, \psi_F, dx_F) = 1$ and hence

$$\varepsilon(\rho, \psi_K, dx_K) = \varepsilon(\phi, \psi_F, dx_F).$$

The remaining character ϕ is ramified; in this case there is an explicit Gauss sum to compute its ε-factor [Tat79, p.14]. One can compute[1] *that with respect to our choices of Haar measures dx_F, dx_K and additive characters*

$$\psi_F(x) = \exp(2\pi\sqrt{-1}\,\mathrm{Tr}_{F/K}\, x), \quad \psi_K(x) = \exp(2\pi\sqrt{-1}x),$$

where Tr *is the trace map and $\sqrt{-1}$ is a fixed element in $\mathbb{C}$, that*

$$\varepsilon(\phi, \psi_F, dx_F) = \varepsilon(\rho, \psi_K, dx_K) = \sqrt{3}.$$

Moreover, one has $W(\rho, \psi_K) = W(\phi, \psi_F) = 1$.

2.3 The ℓ-adic representation of an abelian variety

Definition 2.3.1. *[Roh94, p.147] Let A/K be an abelian variety over a local field. Then the complex Weil–Deligne representation ρ_A is the one associated to the ℓ-adic Galois representation (cf. Proposition 2.1.9) acting on*

$$((\varprojlim_n A[\ell^n]) \otimes \mathbb{Q}_\ell)^* \cong H^1_{\acute{e}t}(A/\overline{K}, \mathbb{Q}_\ell),$$

for any rational prime ℓ different to the residue characteristic of K.[2]

Fact 2.3.2. *[Sab07, Proposition 1.10] Let A/K be an abelian variety over a local field. Then there exists a Galois representation ρ_T and a semisimple Weil–Deligne representation ρ_B such that:*

i. ρ_B has finite image of inertia;

ii. $\rho_B \otimes \chi_{cyc}^{1/2}$ is symplectic;

[1] We choose to omit the calculation here because it is not only an arduous exercise in class field theory, but it is also irrelevant to our later computations.

[2] The corresponding root number is independent of ℓ and choice of embedding $\mathbb{Q}_\ell \hookrightarrow \mathbb{C}$ [Gro72, Théorème 4.3b].

iii. $\rho_T : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_r(\mathbb{Z})$ *for some* $0 \leqslant r \leqslant \dim A$*;*

iv. $\rho_A \cong \rho_B \oplus (\rho_T \otimes \chi_{cyc}^{-1} \otimes \mathrm{sp}(2))$*,*

where χ_{cyc} *and* $\mathrm{sp}(2)$ *are the cyclotomic character and special representation of dimension* 2 *respectively.*

Remark 2.3.3. *In fact, there actually exists an abelian variety* B/K *with potentially good reduction whose associated Weil–Deligne representation is isomorphic to* ρ_B*. Indeed, the finite image of inertia of* ρ_B *is then immediate from the criterion of Néron–Ogg–Shafarevich.*

Definition 2.3.4. *Let* A/K *be an abelian variety and decompose* ρ_A *as in Fact 2.3.2. We say* A/K *has*

i. tame reduction *if* A/L *is semistable for some finite tamely ramified extension* L/K*;*

ii. potentially good reduction *if* ρ_T *is the zero representation;*

iii. potentially totally toric reduction *if* ρ_B *is the zero representation.*

Remark 2.3.5. A/K *is semistable (resp. has tame reduction) if and only if* ρ_B *and* ρ_T *are unramified (resp. tamely ramified); this follows from [Gro72, Proposition 3.5, Corollaire 3.8].*

Definition 2.3.6. *Let* $A/\mathcal{K}$ *be an abelian variety over a global or local field and let* τ *be an Artin representation of* $\mathrm{Gal}(\overline{\mathcal{K}}/\mathcal{K})$*.*

i. If $\mathcal{K} = K$ *is a local field, then the local twisted root number is*

$$W(A/K, \tau) := W(\rho_A \otimes \tau, \psi, dx).$$

ii. If $\mathcal{K}$ *is a global field, then the global twisted root number is*

$$W(A/\mathcal{K}, \tau) := \prod_{v \in M_{\mathcal{K}}} W(A/\mathcal{K}_v, \tau_v),$$

where $M_{\mathcal{K}}$ *is the set of places of* $\mathcal{K}$ *and* τ_v *is the restriction of* τ *to the decomposition group* $\mathrm{Gal}(\overline{\mathcal{K}_v}/\mathcal{K}_v)$ *with respect to the extension of* v *to* $\overline{\mathcal{K}}$*.*

In both cases, we write $W(A/\mathcal{K})$ *for* $W(A/\mathcal{K}, \mathbb{1})$ *and simply refer to this as the (local or global) root number.*

Remark 2.3.7. *Recall that the root number is independent of the choice of Haar mea-*

sure dx. It is also independent of the additive character ψ whenever ρ is symplectic [Roh96, p.315] as we have subtly suggested above. However, we will fix a non-trivial additive character ψ of K to perform our calculations and simply notice that our end results are independent of this choice and hence retain this notation.

2.4 The L-function of an abelian variety

In this section, we recall the construction of the L-function of an abelian variety, as well as its twists by Artin representations. We do this by writing the L-function as an Euler product of L-factors over all places, which in turn use our theory of Weil–Deligne representations.

Definition 2.4.1. *[Roh94, p.137] Let K be a non-Archimedean local field. For a Weil–Deligne representation $\boldsymbol{\rho} = (\rho, N)$ acting on a vector space V, we define the local polynomial to be*

$$P(\boldsymbol{\rho}, T) := \det(1 - \rho(\mathrm{Frob}^{-1})T | V_N^I),$$

where

$$V_N^I = \{v \in V \mid \rho(i)v = v \quad \forall\, i \in I\} \cap \ker N.$$

The corresponding L-factor is

$$L(\boldsymbol{\rho}, s) := P(\boldsymbol{\rho}, q^{-s})^{-1},$$

where q is the cardinality of the residue field of K.

Definition 2.4.2. *Let A/K be an abelian variety over a non-Archimedean local field. We write*

$$L(A/K, s) = L(\rho_A, s)$$

where ρ_A is the Weil–Deligne representation associated to A/K. If τ_v is an Artin representation of $\mathrm{Gal}(\overline{K}/K)$, we define the twisted L-factor

$$L(A/K, \tau_v, s) := L(\rho_A \otimes \tau_v, s)$$

where we identify τ_v with its corresponding Weil–Deligne representation.

Example 2.4.3. *Let $E/\mathbb{Q}_p$ be an elliptic curve, $p < \infty$. If E has good reduction at p, we define $a_p := p + 1 - \tilde{E}(\mathbb{F}_p)$, where $\tilde{E}$ is the reduced curve. Then the local L-factor is*

$$L(E/\mathbb{Q}_p, s) = \begin{cases} (1 - a_p p^{-s} + p^{1-2s})^{-1} & \textit{if } E \textit{ has good reduction}; \\ (1 - p^{-s})^{-1} & \textit{if } E \textit{ has split multiplicative reduction}; \\ (1 + p^{-s})^{-1} & \textit{if } E \textit{ has nonsplit multiplicative reduction}; \\ 1 & \textit{if } E \textit{ has additive reduction}. \end{cases}$$

Definition 2.4.4. *Let $\mathcal{K}$ be a global field and let τ be an Artin representation of $\mathrm{Gal}(\overline{\mathcal{K}}/\mathcal{K})$. For each place v, we extend it to $\overline{\mathcal{K}}$ and define τ_v to be the restriction of τ to the decompostion group at v. We define the global L-functions*

$$\begin{aligned} L(A/\mathcal{K}, s) &= \prod_{v \in M_{\mathcal{K}}, v < \infty} L(A/\mathcal{K}_v, s), \\ L(A/\mathcal{K}, \tau, s) &= \prod_{v \in M_{\mathcal{K}}, v < \infty} L(A/\mathcal{K}_v, \tau_v, s), \end{aligned}$$

where the product runs over all finite places.

Remark 2.4.5. *It is possible to define L-factors at the infinite places $L_\infty(A/\mathcal{K}, s)$ (see for example [Roh94, p.155]) to obtain the completed L-function*

$$\Lambda(A/\mathcal{K}, s) = L_\infty(A/\mathcal{K}, s) L(A/\mathcal{K}, s),$$

although this does not affect the order of vanishing at $s = 1$. If $A = E$ is an elliptic curve of conductor $\mathfrak{N}$ and $\mathcal{K}$ is a number field, then

$$L_\infty(E/\mathcal{K}, s) = (d_{\mathcal{K}}^2 \, \mathrm{Norm}_{\mathcal{K}/\mathbb{Q}} \, \mathfrak{N})^{s/2} (2(2\pi)^{-s} \Gamma(s))^{[\mathcal{K}:\mathbb{Q}]},$$

where $d_{\mathcal{K}}$ is the absolute value of the discriminant of $\mathcal{K}$ and $\Gamma(s) := \int_0^\infty e^{-t} t^{s-1} dt$.

We have defined twisted L-functions for an Artin representation τ. However, we can do several things with Artin representations including direct sums and induction. This should induce relations on the corresponding L-functions; this is known as Artin formalism.

Theorem 2.4.6 (Artin Formalism)**.** *Let $A/\mathcal{K}$ be an abelian variety over a number field and let ρ_1, ρ_2 be Artin representations of $\mathrm{Gal}(\overline{\mathcal{K}}/\mathcal{F})$ for some finite extension $\mathcal{F}/\mathcal{K}$. Then:*

i. (Additivity) $L(A/\mathcal{K}, \rho_1 \oplus \rho_2, s) = L(A/\mathcal{K}, \rho_1, s) L(A/\mathcal{K}, \rho_2, s)$;

ii. (Inductivity) $L(A/\mathcal{K}, \rho_1, s) = L(A/\mathcal{F}, \mathrm{Ind}_{\mathcal{F}/\mathcal{K}} \rho_1, s)$.

For a proof of this theorem for Artin L-functions, see Artin's original German paper [Art23]. The same proofs carry over to the abelian variety setting; for a discussion of the more generalised case see [PRS11, pp. 401-418].

2.5 The Birch–Swinnerton-Dyer and parity conjectures

We shall briefly recap the famous Birch–Swinnerton-Dyer conjecture and its generalisation to Artin twists which forms the motivation for the majority of this thesis, as well as giving an overview of the current progress.

Theorem 2.5.1 (Mordell–Weil, Lang–Néron)**.** *Let $A/\mathcal{K}$ be an abelian variety over a global field. Then the set $A(\mathcal{K})$ of $\mathcal{K}$-rational points is a finitely generated abelian group. Explicitly there is some integer $r \geqslant 0$ and finite torsion group T such that*

$$A(\mathcal{K}) \cong \mathbb{Z}^r \times T.$$

The rank of $A/\mathcal{K}$, $\operatorname{rk} A/\mathcal{K}$, is the integer r above.

The essence of the Birch–Swinnerton-Dyer conjecture is that it relates the rank of $A/\mathcal{K}$, a purely algebraic invariant, to the analytic L-function.

Conjecture 2.5.2 (Birch–Swinnerton-Dyer [BSD63, BSD65, Tat66])**.** *Let $A/\mathcal{K}$ be an abelian variety over a global field. Then $L(A/\mathcal{K}, s)$ has analytic continuation to the entire complex plane and*

$$\operatorname{rk} A/\mathcal{K} = \operatorname{ord}_{s=1} L(A/\mathcal{K}, s).$$

The analytic continuation statement is required to ensure that the order of vanishing at $s = 1$ is well-defined; a priori the L-function only converges on some right half plane, i.e. for $\Re(s) \gg 0$. When $A = E$ is an elliptic curve, we do have analytic continuation if:

i. E has complex multiplication (see for example [Sil13, Theorem II.10.5]);

ii. $\mathcal{K} = \mathbb{Q}$ or a real quadratic field due to modularity results [Wil95, TW95, BCDT01, FLS15].

For this reason most of the progress of the Birch–Swinnerton-Dyer conjecture has been done for elliptic curves over $\mathbb{Q}$. The following theorem is a culmination of work done

by Coates–Wiles, Gross–Zagier and Kolyvagin [CW77, GZ86, Kol88].

Theorem 2.5.3. *Let $E/\mathbb{Q}$ be an elliptic curve and suppose that $\operatorname{ord}_{s=1} L(E/\mathbb{Q}, s) \leqslant 1$. Then the Birch–Swinnerton-Dyer conjecture holds.*

A simpler approach is to consider the parity conjecture; this will be our main focus. To motivate this we use the Hasse–Weil conjecture.

Conjecture 2.5.4 (Hasse–Weil)**.** *Let $A/\mathcal{K}$ be an abelian variety over a global field. Then the completed L-function $\Lambda(A/\mathcal{K}, s)$ has analytic continuation to the entire complex plane and satisfies a functional equation of the form*

$$\Lambda(A/\mathcal{K}, s) = w(A/\mathcal{K})\Lambda(A/\mathcal{K}, 2 - s)$$

for some $w(A/\mathcal{K}) \in \{\pm 1\}$, the "sign of the functional equation" (which we are intentionally distinguishing from the root number $W(A/\mathcal{K})$; see Remark 2.5.6).

Remark 2.5.5. *The Hasse–Weil conjecture is implied by the current modularity results so is therefore true for elliptic curves over $\mathbb{Q}$.*

Observe that if $\Lambda(A/\mathcal{K}, 1) \neq 0$, then we necessarily have $w(A/\mathcal{K}) = 1$. If the order of vanishing is 1, then by differentiating we see that $w(A/\mathcal{K}) = -1$. More generally, we notice that

$$w(A/\mathcal{K}) = (-1)^{\operatorname{ord}_{s=1} \Lambda(A/\mathcal{K}, s)}.$$

Remark 2.5.6. *The sign in the functional equation $w(A/\mathcal{K})$ is conjectured to equal the global root number $W(A/\mathcal{K})$ (see for example [Roh94, p.157]) which lends creedence to the term "expected sign of the functional equation".*

We would like to invoke the Birch–Swinnerton-Dyer conjecture to say that $w(A/\mathcal{K}) = (-1)^{\operatorname{rk} A/\mathcal{K}}$; but this still relies on the Hasse–Weil conjecture to make sense. Instead, we use the global root number to remove all conjectural dependency on the L-function.

Conjecture 2.5.7 (Parity conjecture)**.** *Let $A/\mathcal{K}$ be an abelian variety over a global field with global root number $W(A/\mathcal{K})$. Then*

$$W(A/\mathcal{K}) = (-1)^{\operatorname{rk} A/\mathcal{K}}.$$

Corollary 2.5.8. *Assume the parity conjecture for $A/\mathcal{K}$. If $W(A/\mathcal{K}) = -1$, then $\operatorname{rk} A/\mathcal{K}$ is odd and in particular positive; this implies that $A(\mathcal{K})$ is infinite.*

Theorem 2.5.9. *[DD11, Theorem 1.2] Let $E/\mathcal{K}$ be an elliptic curve over a number*

field and assume the Tate–Shafarevich group is finite. Then the parity conjecture holds for $E/\mathcal{K}$.

Now we consider the generalisation of these conjectures to Artin twists which we will use the twisted L-function. Let τ be an Artin representation which factors through $\mathrm{Gal}(\mathcal{F}/\mathcal{K})$ for some finite Galois extension $\mathcal{F}/\mathcal{K}$.

For an abelian variety $A/\mathcal{K}$, consider the set

$$A(\mathcal{F})_{\mathbb{C}} := A(\mathcal{F}) \otimes_{\mathbb{Z}} \mathbb{C} \cong \mathbb{C}^{\mathrm{rk}\, A/\mathcal{F}}.$$

The Galois action on the points of $A(\mathcal{F})$ gives $A(\mathcal{F})_{\mathbb{C}}$ the structure of a $\mathbb{C}[\mathrm{Gal}(\mathcal{F}/\mathcal{K})]$-module; we identify this with the corresponding representation.

Example 2.5.10. *Consider the elliptic curve $E/\mathbb{Q} : y^2+y = x^3-x^2-7820x-263580$ (Cremona label 11a2) and let $\mathcal{F} = \mathbb{Q}(\sqrt{2})$. Then $E(\mathcal{F})_{\mathbb{C}} \cong \mathbb{C}$ is 1-dimensional, generated by $P = (\frac{267617}{1058}, \frac{-128202697\sqrt{2}-24334}{48668})$. Since $E(\mathbb{Q})$ has rank 0, the Artin representation on $E(\mathcal{F})_{\mathbb{C}}$ is isomorphic to the quadratic character η that factors through $\mathrm{Gal}(\mathcal{F}/\mathbb{Q})$.*

Indeed, if $E/\mathbb{Q}$ is an arbitrary elliptic curve then $E(\mathcal{F})_{\mathbb{C}} \cong E(\mathbb{Q})_{\mathbb{C}} \oplus E^{\eta}(\mathbb{Q})_{\mathbb{C}}$, where E^{η} is the quadratic twist of E by η; this is the arithmetic interpretation of the analytic statement

$$L(E/\mathcal{F}, s) = L(E/\mathbb{Q}, s)L(E^{\eta}/\mathbb{Q}, s),$$

where we note that we have an isomorphism of Tate modules $T_\ell E^{\eta} \cong T_\ell E \otimes \eta$.

Conjecture 2.5.11 (Birch–Swinnerton-Dyer, Deligne–Gross; see [Roh90] p.127)**.** *Let $A/\mathcal{K}$ be an abelian variety over a global field and let τ be an Artin representation of $\mathrm{Gal}(\mathcal{F}/\mathcal{K})$ for some finite Galois extension $\mathcal{F}/\mathcal{K}$. Then $L(A/\mathcal{K}, \tau, s)$ has analytic continuation to $\mathbb{C}$ and*

$$\mathrm{ord}_{s=1}\, L(A/\mathcal{K}, \tau, s) = \langle A(\mathcal{F})_{\mathbb{C}}, \tau \rangle.$$

This conjecture is simply the natural extension of the Birch–Swinnerton-Dyer conjecture using Artin formalism. If we let $\tau = \mathbb{1}_{\mathcal{K}}$, then we recover the original Birch–Swinnerton-Dyer conjecture: $\langle A(\mathcal{F})_{\mathbb{C}}, \mathbb{1}_{\mathcal{K}} \rangle$ is equal to the number of linearly independent points that are defined over $\mathcal{K}$, i.e. $\mathrm{rk}\, A/\mathcal{K}$. We are also able to recover that $\mathrm{rk}\, A/\mathcal{F} = \langle A(\mathcal{F})_{\mathbb{C}}, \mathrm{Ind}_{\mathcal{F}/\mathcal{K}}\, \mathbb{1}_{\mathcal{F}} \rangle$ as a sum of multiplicities of Artin twists, corresponding to the fact that the base changed L-function $L(A/\mathcal{F}, s)$ is a product of twisted

L-functions $L(A/\mathcal{K}, \tau, s)$.

In the example above, we looked at part of this statement when $\mathcal{F}/\mathcal{K}$ was quadratic; the non-trivial character of $\mathrm{Ind}_{\mathcal{F}/\mathcal{K}} \mathbb{1}_{\mathcal{F}}$ measured the rank of the quadratic twist instead. Note that each summand of $\mathrm{Ind}_{\mathcal{F}/\mathcal{K}} \mathbb{1}_{\mathcal{F}}$ occurs to its dimension; this ensures that we count $\mathrm{rk}\, A/\mathcal{F}$ correctly as a d-dimensional representation requires d linearly independent points to exist.

The completed twisted L-function should also satisfy a functional equation of the form

$$\Lambda(A/\mathcal{K}, \tau, s) = w(A/\mathcal{K}, \tau)\Lambda(A/\mathcal{K}, \tau^*, 2 - s).$$

This time however, we only have $|w(A/\mathcal{K}, \tau)| = 1$; we need to impose that τ is self-dual (i.e. $\tau \cong \tau^*$) in order to ensure $w(A/\mathcal{K}, \tau) \in \{\pm 1\}$.

Conjecture 2.5.12 (Twisted parity conjecture)**.** *Let $A/\mathcal{K}$ be an abelian variety over a global field and let τ be a self-dual Artin representation of $\mathrm{Gal}(\mathcal{F}/\mathcal{K})$ for some finite Galois extension $\mathcal{F}/\mathcal{K}$. Then*

$$W(A/\mathcal{K}, \tau) = (-1)^{\langle A(\mathcal{F})_{\mathbb{C}}, \tau \rangle}.$$

Chapter 3

Root numbers of abelian varieties

3.1 Introduction

Our main objective in this chapter is to give explicit formulae for calculating the global root number of abelian varieties with tame reduction, building on work of Rohrlich. The global root number is conjecturally equal to the sign of the functional equation and hence controls the parity of the analytic rank. This has two computational uses: numerically verifying the parity conjecture; and checking for infinitely many points, since a negative root number implies odd rank. We do this by explicitly computing each local root number and writing them as a product of Jacobi symbols, analogously to the elliptic curve case.

As an example we use our formulae to compute the global root number of the Jacobian of several hyperelliptic curves in §3.4, using results of [DDMM]. This also enables us to recover the root numbers computed in a recent paper of Brumer, Kramer and Sabitova [BKS18].

For reference, we give Rohrlich's result for root numbers of elliptic curves in terms of Jacobi symbols. This is the result we will generalise to abelian varieties.

Theorem 3.1.1. *[Roh96, Theorem 2] Let K be a finite extension of $\mathbb{Q}_p$ with normalised valuation v and residue field of cardinality q. Let E/K be an elliptic curve and let j, Δ_E denote the j-invariant and discriminant of E respectively.*

i. If $v(j) < 0$ and $p \geqslant 3$, then

$$W(E/K) = \begin{cases} -1 & \textit{if } E/K \textit{ has split multiplicative reduction;} \\ 1 & \textit{if } E/K \textit{ has nonsplit multiplicative reduction;} \\ \left(\frac{-1}{q}\right) & \textit{otherwise.} \end{cases}$$

ii. If $v(j) \geqslant 0$ *and* $p \geqslant 5$*, set* $e = \dfrac{12}{\gcd(v(\Delta_E), 12)}$*. Then*

$$W(E/K) = \begin{cases} 1 & \textit{if } e = 1; \\ \left(\frac{-1}{q}\right) & \textit{if } e = 2 \quad \textit{or } e = 6; \\ \left(\frac{-3}{q}\right) & \textit{if } e = 3; \\ \left(\frac{-2}{q}\right) & \textit{if } e = 4. \end{cases}$$

3.1.1 Notation and main result

We now set up some notation that we frequently use throughout the next two chapters, in addition to that given in §1.1. For definitions of the root number of a representation, reduction types of an abelian variety and ρ_A see §2. Unless otherwise specified, we shall suppose throughout that ρ_A is tamely ramified, i.e. the image of wild inertia is trivial; this is always true if $p > 2 \dim A + 1$ [ST68, p.497].

Notation.

ψ	a non-trivial additive character of K,
$n(\psi)$	the conductor of ψ,
A/K	an abelian variety,
ρ_A	$\cong \rho_B \oplus (\rho_T \otimes \chi_{cyc}^{-1} \otimes \mathrm{sp}(2))$ the canonical ℓ-adic representation of A/K, where ρ_B, ρ_T have finite image of inertia (cf. Fact 2.3.2),
$\tilde{\varphi}(e)$	$= \begin{cases} 2 & \text{if } e = 1, 2, \\ \lvert\,(\mathbb{Z}/e\mathbb{Z})^\times\,\rvert & \text{if } e \geqslant 3, \end{cases}$
$m_e \in \mathbb{Z}$	$= \lvert\{\text{eigenvalues of } \rho_B(\iota) \text{ of order } e\}\rvert/\tilde{\varphi}(e)$ (counting multiplicity) for each positive integer e,
m_T	multiplicity of -1 as an eigenvalue of $\rho_T(\iota)$,
$\left(\frac{*}{*}\right)$	the Jacobi symbol.

We now detail the main result of the chapter. We are fortunate to once again be able to write the local root number compactly as a product of Jacobi symbols.

Theorem 3.1.2 (=Theorem 3.3.5)**.** *Let A/K be an abelian variety over a non-Archimedean local field which has tame reduction. Then*

$$W(A/K) = \left(\prod_{e \in \mathbb{N}} W_{q,e}^{m_e} \right) (-1)^{\langle \mathbb{1}, \rho_T \rangle} W_{q,2}^{m_T},$$

where for an integer $k > 0$ and rational odd prime l:

$$W_{q,e} = \begin{cases} \left(\frac{q}{l}\right) & \text{if } e = l^k; \\ \left(\frac{-1}{q}\right) & \text{if } e = 2l^k \quad \text{and } l \equiv 3 \bmod 4 \qquad \text{or } e = 2; \\ \left(\frac{-2}{q}\right) & \text{if } e = 4; \\ \left(\frac{2}{q}\right) & \text{if } e = 2^k \quad \text{for } k \geqslant 3; \\ 1 & \text{else.} \end{cases}$$

Remark 3.1.3. *When $A = E$ is an elliptic curve, our result coincides with Rohrlich's.*

The layout of this chapter is as follows. In §3.2 we study the local root number of a symplectic Weil representation ρ; this includes the Weil–Deligne representation ρ_B associated to an abelian variety with potentially good reduction. We do this in four stages:

i. study irreducible tame Artin representations (§3.2.1);

ii. compute root numbers of irreducible Weil representations depending on whether they are self-dual or not (§3.2.2-3);

iii. show that ρ be decomposed into summands of a specific form (§3.2.4);

iv. derive a Jacobi symbol for each representation of this form (§3.2.5).

In §3.3, we then study root numbers of indecomposable Weil–Deligne representations which are not semisimple; this determines the root number corresponding to an Artin twist of $\mathrm{sp}(2)$. Since root numbers are additive, we are then able to prove our main theorem above.

With this theory in hand, we close the chapter by giving some worked examples in §3.4, where the abelian variety will arise as the Jacobian of a hyperelliptic curve. We use work of Dokchitser, Dokchitser, Maistret and Morgan [DDMM] to obtain the relevant data needed to apply our results.

3.2 Potentially good reduction

3.2.1 Decomposition of the representation

We first study the Weil–Deligne representation ρ_B which can be identified with a representation of the Weil group with finite image of inertia.

Our assumption that ρ_A (and hence also ρ_B) is tamely ramified implies that p will necessarily be coprime to the order of the image of the inertia group. We shall want to deal with the irreducible summands of ρ_B so our first step in that direction is the following easy lemma about $\rho_B(I)$, which follows directly from the structure of the Weil group.

Lemma 3.2.1. *Let $\rho : \mathcal{W}(\overline{K}/K) \to \mathrm{GL}(V)$ be a tamely ramified representation with finite image of inertia. Suppose the characteristic polynomial of $\rho(\iota)$ has coefficients in $\mathbb{Z}$. If the characteristic polynomial is reducible (over $\mathbb{Z}$) into a product of two coprime polynomials, then ρ is also reducible as a Weil representation.*

Proof. Let ι be a generator of tame inertia and note that all eigenvalues of $\rho(\iota)$ are roots of unity. For $\lambda \in \mathbb{C}$, define $V_\lambda = \{v \in V \mid \iota v = \lambda v\}$ to be the associated eigenspace. We claim that $\mathrm{Frob}^{-1} V_{\zeta_e} = V_{\zeta_e^q}$. To see this, recall the action of the semidirect product of Frobenius on the tame inertia group is $\mathrm{Frob} \cdot \iota \cdot \mathrm{Frob}^{-1} = \iota^q$.

Now let $v \in V_{\zeta_e}$. Then

$$\begin{aligned} \mathrm{Frob}\, \iota\, \mathrm{Frob}^{-1}\, v &= \iota^q v = \zeta_e^q v, \\ \iota\, \mathrm{Frob}^{-1}\, v &= \mathrm{Frob}^{-1}\, \zeta_e^q v = \zeta_e^q\, \mathrm{Frob}^{-1}\, v, \end{aligned}$$

and hence $\mathrm{Frob}^{-1}\, v \in V_{\zeta_e^q}$.

Let $W = \bigoplus_{(k,e)=1} V_{\zeta_e^k}$. By the assumption on the reducibility of the characteristic polynomial of $\rho(\iota)$, we necessarily have two primitive roots of distinct order as eigenvalues for ι and hence $W \neq V$. However, W is an invariant subspace since Frob fixes each summand and ι permutes them. Hence ρ is reducible as claimed. □

Therefore by decomposing ρ_B if necessary, we may assume that the eigenvalues of $\rho_B(\iota)$ are all primitive e^{th} roots of unity for some fixed e. The irreducible summands of ρ_B are one-dimensional unramified twists of representations of Galois type (cf. Theorem 2.1.13).

Definition 3.2.2. *Let $\rho : \mathcal{W}(\overline{K}/K) \to \mathrm{GL}(V)$ be a Weil representation. Then ρ is said to be of Galois type if it factors through an open subgroup of finite index. Equivalently, there exists a finite Galois extension L/K such that ρ is trivial on $\mathcal{W}(\overline{K}/L)$ so that ρ has finite image.*

Note $\dfrac{\mathcal{W}(\overline{K}/K)}{\mathcal{W}(\overline{K}/L)} \cong \mathrm{Gal}(L/K)$ so we may (and freely do so) identify representations of Galois type with Artin representations. We therefore study Artin representations which factor through a finite Galois extension. Since we assume that ρ_B is tamely ramified, we shall only concern ourselves with the case when L/K is tamely ramified. Since the tame quotient is isomorphic to $\langle \iota \rangle \rtimes \langle \mathrm{Frob} \rangle$, we may assume that our Artin representations factor (not necessarily faithfully) through a tame Galois extension L/K with

$$\mathrm{Gal}(L/K) = \langle \iota, \mathrm{Frob} \,|\iota^e, \mathrm{Frob}^n, \mathrm{Frob}\, \iota\, \mathrm{Frob}^{-1} = \iota^q \rangle \cong C_e \rtimes C_n,$$

where e, n are the ramification and residue degrees of L/K respectively. Note that the order f of $q \bmod e$ necessarily divides n. Moreover, we may suppose that the Artin representation θ is faithful on the inertia subgroup since by factoring through the kernel of θ restricted to inertia, we still obtain a split extension of this form.

Notation. *Throughout the remainder of this section, we let θ denote an irreducible, Artin representation of $\mathrm{Gal}(L/K) = \langle \iota, \mathrm{Frob} \,|\iota^e, \mathrm{Frob}^n, \mathrm{Frob}\, \iota\, \mathrm{Frob}^{-1} = \iota^q \rangle$, where, $p \nmid e$, $\mathrm{Aut}_{\langle \mathrm{Frob} \rangle}(\langle \iota \rangle) \cong C_f$ (i.e. $q \bmod e$ has order f) and we suppose that $f > 1$ and hence $e > 2$.*

Lemma 3.2.3. *Let θ be an irreducible, tamely ramified representation of $\mathrm{Gal}(L/K)$ which is faithful on the inertia subgroup. Then:*

i. $\dim \theta = f$;

ii. $\theta = \mathrm{Ind}_{\langle \iota, \mathrm{Frob}^f \rangle}^{\mathrm{Gal}(L/K)} \chi \otimes \gamma$ *where χ is a character of $\langle \iota \rangle$, γ is a character of $\langle \mathrm{Frob}^f \rangle$;*

iii. $(\det \theta)(\iota) = \chi\left(\iota^{\frac{q^f-1}{q-1}}\right), \quad (\det \theta)(\mathrm{Frob}) = (-1)^{1+\dim \theta} \gamma(\mathrm{Frob}^f)$;

iv. *θ is self-dual if and only if f is even, $q^{f/2} \equiv -1 \bmod e$ and $\gamma^2 = \mathbb{1}$. Moreover, if θ is self-dual, then it factors faithfully through $\mathrm{Gal}(L/K)/\ker \gamma$;*

v. *if θ is self-dual, then θ is orthogonal if and only if $\gamma = \mathbb{1}$;*

vi. *the Artin conductor exponent of $\theta \otimes \nu$ is equal to f for any one dimensional unramified character ν of $\mathcal{W}(\overline{K}/K)$.*

Proof. (i), (ii): We use [Ser77, p.62] which completely describes the irreducible representations of such a group. Let χ be a character of $\langle \iota \rangle$ and let γ be a character of $\mathrm{Stab}(\chi) = \{\mathrm{Frob}^k \mid \chi(\mathrm{Frob}^{-k}\, \iota\, \mathrm{Frob}^k) = \chi(\iota)\}$. Then $\theta = \mathrm{Ind}_{\langle \iota \rangle \rtimes \mathrm{Stab}(\chi)}^{\mathrm{Gal}(L/K)} \chi \otimes \gamma$ is irreducible and all such irreducible representations of $\mathrm{Gal}(L/K)$ arise this way.

We now claim that χ is necessarily faithful. By Mackey's formula, we have

$$\mathrm{Res}_{\langle \iota \rangle}^{\mathrm{Gal}(L/K)}\, \theta(\iota) = \bigoplus_{k=1}^{\dim \theta} {}^{\mathrm{Frob}^k}\chi(\iota),$$

where ${}^{\mathrm{Frob}^k}\chi(\iota) := \chi(\mathrm{Frob}^{-k}\, \iota\, \mathrm{Frob}^k)$. If χ has order $d < e$, then ${}^{\mathrm{Frob}^k}\chi(\iota^d) = 1$ for all k (since conjugates have the same order) and hence θ is not faithful on the inertia subgroup. This implies γ is a character of $\mathrm{Stab}(\chi) = \langle \mathrm{Frob}^f \rangle$.

(iii): We can now explicitly compute the induced representation θ in terms of χ and γ. Indeed, choosing coset representatives Frob^{-j} for $\mathrm{Gal}(L/K)/\langle \iota, \mathrm{Frob}^f \rangle$ we compute that:

$$\theta(\iota) = \begin{pmatrix} \chi(\iota) & & & \\ & \chi(\iota^q) & & \\ & & \ddots & \\ & & & \chi(\iota^{q^{f-1}}) \end{pmatrix}, \theta(\mathrm{Frob}) = \begin{pmatrix} & & & \gamma(\mathrm{Frob}^f) \\ 1 & & & \\ & \ddots & & \\ & & 1 & \end{pmatrix},$$

where we have only indicated the nonzero entries; the determinant now follows.

(iv): Recall that θ is self-dual if and only if it has real trace. First note that $\theta(\mathrm{Frob}^f) = \gamma(\mathrm{Frob}^f) I$ is scalar and hence $\gamma(\mathrm{Frob}^f) \in \{\pm 1\}$ so $\gamma^2 = \mathbb{1}$. Now let $\chi(\iota) = \zeta_e$. Then the trace of $\theta(\iota)$ is $\sum_{k=0}^{f-1} \zeta_e^{q^k}$; this is real if and only if it is fixed under complex conjugation. As each term is a primitive e^{th} root of unity, this is equivalent to saying that there exists $l \in \mathbb{Z}$ such that $\zeta_e^{q^l} = \zeta_e^{-1}$, i.e. $q^l \equiv -1 \bmod e$; from this we determine that f is even and moreover we must have $q^{f/2} \equiv -1 \bmod e$. Lastly, observe that $\theta(\mathrm{Frob}^n\, \iota^k)$ has trace zero unless $f|n$; when $f|n$ the above computations show that we have real trace and hence our criteria are sufficient for θ to be self-dual.

To note that θ is faithful on $\mathrm{Gal}(L/K)/\ker \gamma$, note that $\theta(\iota^a\, \mathrm{Frob}^b)$ is not diagonal unless $f|b$. As θ is faithful on inertia, this implies $\ker \theta \subset \langle \mathrm{Frob}^f \rangle$ so this now follows as $\theta(\mathrm{Frob}^f) = \gamma(\mathrm{Frob}^f)^{\oplus f}$.

(v): Recall that irreducible self-dual representations are either orthogonal or symplec-

tic. Since symplectic representations have trivial determinant, it is straightforward to see that θ is orthogonal if $\gamma = \mathbb{1}$. The case $\gamma \neq \mathbb{1}$ is the content of [Sab07, Proposition 1.5]; see Proposition 4.2.1 for the statement.

(vi): Observe that $\theta \otimes \nu$ has no inertia invariant subspace and so a direct computation shows that the Artin conductor exponent is equal to $\dim(\theta \otimes \nu) = f$. □

Lemma 3.2.4. *Let ρ be a symplectic Weil representation which has finite image of inertia and let π be a 1-dimensional summand of ρ. Then there exists another distinct 1-dimensional summand $\tilde{\pi}$ of ρ such that $\tilde{\pi} \cong \pi^*$.*

Proof. Take V to be the complex vector space on which ρ acts and W to be the subspace corresponding to π. Let $\operatorname{Ann} W$ be the annihilator of W with respect to the symplectic pairing. By the properties of dual spaces, we have $(V/W)^* \cong \operatorname{Ann} W$.

As symplectic pairings are alternating, $W \subset \operatorname{Ann} W$ and there exists a distinct subrepresentation $\tilde{\pi}$ of ρ on V/W such that $\tilde{\pi}^* \cong \pi$. □

We now individually separate into two cases dependent on whether our irreducible Weil representation is self-dual or not; our method for computing the root number is different in each case.

3.2.2 Dual pairs

We first consider the irreducible Weil representations which are not self-dual. We first show that in our context, such representations must arise in pairs. Computation of the corresponding root number will then be straightforward with the aid of Corollary 2.2.6.

Lemma 3.2.5. *Let ρ be a self-dual Weil representation and let σ be an irreducible summand of ρ which is not self-dual. Then σ^* is a distinct irreducible summand of ρ.*

Proof. Observe that since ρ is self-dual, σ^* is an irreducible summand of ρ. Since σ is not self-dual, it is necessarily distinct to σ. □

Remark 3.2.6. *Lemma 3.2.4 tells us that this also holds for self-dual characters (which have order dividing 2 on inertia) so we shall deal with all characters under this case and assume $\dim \rho \geqslant 2$ in the self-dual setting. This is the reason for our definition of $\tilde{\varphi}$; such self-dual characters will appear with even multiplicity so our tweak of the usual Euler totient function takes this into account.*

Remark 3.2.7. *If A/K has good reduction, then $\rho_A = \rho_B$ splits as a sum of unramified characters and hence $W(A/K, \psi) = 1$.*

Before we examine $\det \sigma$ in more detail, we shall first turn our attention to the Artin map. This enables us to identify $\det \sigma$ with a character ϕ of $K^\times$, where the inertia group corresponds to the unit group $\mathcal{O}_K^\times$. Since the image of inertia is finite, we are able to discuss the (necessarily finite) order of ϕ on inertia. In addition, ϕ is at most tamely ramified; it may actually be unramified (and therefore has order 1) but the criterion we shall shortly give will take this into account.

The subgroup of wild inertia is identified with the group of principal units and hence we can factor our character through this to get a character on the torsion subgroup consisting of elements with order coprime to p, which is isomorphic to the units of the residue field. It is this new character that we now deal with; we shall freely swap between the two interpretations, as in the following composition:

$$\phi : \mathcal{O}_K^\times \twoheadrightarrow \frac{\mathcal{O}_K^\times}{1 + \pi_K \mathcal{O}_K} \cong \mathbb{F}_q^\times \to \mathbb{C}^\times.$$

Lemma 3.2.8. *Let $q \equiv 1 \bmod r$ and $\phi : K^\times \to \mathbb{C}^\times$ be a tamely ramified character such that $\phi(\mathcal{O}_K^\times)$ is cyclic of order r. If q is even, then $\phi(-1) = 1$. Otherwise q is odd and*

$$\phi(-1) = 1 \Leftrightarrow q \equiv 1 \bmod 2r.$$

Proof. If q is even, then r is necessarily odd (as ϕ is tamely ramified). Then $\phi(-1) = \phi((-1)^r) = \phi^r(-1) = 1$.

Now suppose q is odd. By considering the action of ϕ on the residue field, we note that $\phi(x) = 1 \Leftrightarrow x \in \left(\mathbb{F}_q^\times\right)^r$, and hence we only need to ascertain whether $-1 \in \left(\mathbb{F}_q^\times\right)^r$.

Let ξ be a generator of $\mathbb{F}_q^\times$ and note $-1 = \xi^k$ where $q - 1 = 2k$. Then

$$\begin{aligned} -1 \in \left(\mathbb{F}_q^\times\right)^r &\Leftrightarrow r | k, \\ &\Leftrightarrow 2r | (q-1). \end{aligned}$$

□

We shall now consider $\det \sigma$ explicitly to get a closed form expression for the corresponding root number. From Lemma 3.2.3iii, $(\det \sigma)(\iota) = \zeta_e^{\frac{q^f - 1}{q-1}}$ since χ is faithful. This implies that $(\det \sigma)(\mathcal{O}_K^\times)$ is cyclic of order $r = \dfrac{e}{\gcd(e, \frac{q^f-1}{q-1})}$. The following

lemma shows that the congruence hypothesis on q is satisfied whenever q is odd.

Lemma 3.2.9. *Let $e > 0$, q a power of an odd prime, f the least positive integer such that $q^f \equiv 1 \bmod e$. Then $q \equiv 1 \bmod \dfrac{e}{\gcd(e, \frac{q^f-1}{q-1})}$.*

Proof. First recall that $\gcd(ab, c) = \gcd(a, c)\gcd(b, c)$ whenever $\gcd(a, b) = 1$. This means it suffices to prove the lemma when e is a prime power.

Let $e = l^k$ for some prime l and let $m = v_l(q-1)$ be the l-adic valuation. Then $v_l(\frac{q^f-1}{q-1}) \geqslant k-m$. Hence $\gcd(e, \frac{q^f-1}{q-1}) \geqslant l^{k-m}$ so $\dfrac{e}{\gcd(e, \frac{q^f-1}{q-1})} \leqslant l^m$. Since $v_l(q-1) = m$, the result holds. □

The above two lemmas, in conjunction with Corollary 2.2.6, now provide the proof for the following theorem.

Theorem 3.2.10. *Let σ be a tamely-ramified irreducible f-dimensional Weil representations such that $|\sigma(I)| = e$ is finite. If q is even then $W(\sigma \oplus \sigma^*, \psi) = 1$. Otherwise*

$$W(\sigma \oplus \sigma^*, \psi) = 1 \Leftrightarrow q \equiv 1 \bmod \frac{2e}{\gcd(e, \frac{q^f-1}{q-1})}.$$

Remark 3.2.11. *If $\dim \sigma = 1$ and q is odd, then $W(\sigma \oplus \sigma^*, \psi) = 1 \Leftrightarrow q \equiv 1 \bmod 2e$.*

Remark 3.2.12. *Observe that if e is odd, then $W(\sigma \oplus \sigma^*, \psi) = 1$ independently of whether q is odd or even.*

3.2.3 The self-dual case

In this section, we study irreducible self-dual Weil representations. Our first step is to show that they may be identified with Artin representations.

Lemma 3.2.13. *Let ρ be an irreducible self-dual Weil representation. Then ρ is of Galois type and hence isomorphic to an Artin representation.*

Proof. Observe that by the classification of Weil representations (Theorem 2.1.13), $\rho \cong \theta \otimes \nu$ for some Artin representation θ and unramified character ν. Hence $\theta \otimes \nu \cong \theta^* \otimes \nu^{-1}$ and so $\theta \cong \theta^* \otimes \nu^{-2}$. Now $\det \theta = (\det \theta)^{-1} \otimes \nu^{-2\dim\theta}$ and hence $\nu^{2\dim\theta} = (\det\theta)^2$. Since θ is an Artin representation, $\det\theta$ has finite order and hence so does ν. Therefore ρ is of Galois type. □

The above lemma enables us to directly apply the results of Lemma 3.2.3, which we shall do frequently. Since we have already dealt with the self-dual characters, we suppose that $\dim\theta = f \geqslant 2$. Recall that θ has the form $\theta = \mathrm{Ind}_H^G \chi \otimes \gamma$, where $H = \langle \iota, \mathrm{Frob}^f \rangle \leq G = \mathrm{Gal}(L/K)$. As θ is a monomial representation, we use the inductivity property of ε-factors; we carefully select a suitable representation to ease our computation.

To apply Theorem 2.2.1ii, we need to choose an auxiliary character of H to $\chi \otimes \gamma$; the obvious choice here is the trivial character $\mathbb{1}_H$. This has several benefits as we shall see. Firstly, its induction is simply the permutation action on the cosets of H. In other words, $\mathrm{Ind}_H^G \mathbb{1}_H = \mathbb{C}[G/H]$, but since G/H is an abelian group, the induction must also split as a sum of characters. Moreover, these summands are unramified since their restriction to inertia is the trivial character by Frobenius reciprocity.

We will also need to compute their associated root numbers; for that we use the self-duality of the trivial character and its induction.

Lemma 3.2.14. *Let G be a group, $N \leqslant G$ a subgroup and let M be a self-dual $\mathbb{C}[N]$ module, i.e. $M^* \cong M$. Then $M \otimes_{\mathbb{C}[N]} \mathbb{C}[G]$ is also self-dual.*

Proof. Since $\mathbb{C}[G]$ is self-dual, $(M \otimes_{\mathbb{C}[N]} \mathbb{C}[G])^* = M^* \otimes_{\mathbb{C}[N]} \mathbb{C}[G]^* = M \otimes_{\mathbb{C}[N]} \mathbb{C}[G]$. □

By the above lemma, $\mathrm{Ind}_H^G \mathbb{1}_H$ is self-dual. The only self-dual characters which are trivial on H are the trivial character and the sign of the permutation representation on G/H, which we shall write as $\mathrm{sign}_{[G:H]}$. Applying Frobenius reciprocity again and considering dimensions, we note that these occur exactly once. The remaining summands must all then occur in pairs with their dual. This leads us to following result.

Lemma 3.2.15. *Let L/K be a finite Galois extension with Galois group G, $H \leqslant G$ a subgroup containing the inertia subgroup and let $\mathrm{sign}_{[G:H]}$ be the sign of the permutation representation*[1] *on G/H. Then*

$$W(\mathrm{Ind}_H^G \mathbb{1}_H, \psi) = W(\mathrm{sign}_{[G:H]}, \psi).$$

Proof. Observe that $\mathrm{Ind}_H^G \mathbb{1}_H = \mathbb{1}_G^t \oplus \mathrm{sign}_{[G:H]} \oplus \bigoplus_{j=1}^k (\chi_j \oplus \chi_j^*)$ where χ_j are unramified one-dimensional representations, $t \in \{0, 1\}$ is positive if and only if $|G/H|$ is

[1] This is the trivial representation if $|G/H|$ is odd.

even. Now by Corollary 2.2.6, $W(\chi_j \oplus \chi_j^*, \psi) = \chi_j(-1) = 1$, and a direct computation shows $W(\mathbb{1}_G, \psi) = 1$. □

The inductivity property (Theorem 2.2.1ii) for root numbers gives us

$$\frac{W(\theta, \psi)}{W(\mathrm{Ind}_H^G \mathbb{1}_H, \psi)} = \frac{W(\chi \otimes \gamma, \psi \circ \mathrm{Tr}_{L^H/K})}{W(\mathbb{1}_H, \psi \circ \mathrm{Tr}_{L^H/K})},$$

and so using the above we have reduced this to $W(\theta, \psi) = W(\mathrm{sign}_{[G:H]}, \psi) W(\chi \otimes \gamma, \psi \circ \mathrm{Tr}_{L^H/K})$ since $W(\mathbb{1}_H, \psi \circ \mathrm{Tr}_{L^H/K}) = 1$.

Lemma 3.2.16. *Assume $[G : H]$ is even and that H contains the inertia subgroup. Then $W(\mathrm{sign}_{[G:H]}, \psi) = (-1)^{n(\psi)}$.*

Proof. By Theorem 2.2.1, we get that $W(\mathrm{sign}_{[G:H]}, \psi) = \mathrm{sign}_{[G:H]}(\pi_K^{n(\psi)})$. Since $\mathrm{sign}_{[G:H]}$ is an unramified quadratic character, we necessarily have $\mathrm{sign}_{[G:H]}(\pi) = -1$ and hence $W(\mathrm{sign}_{[G:H]}, \psi) = (-1)^{n(\psi)}$. □

Remark 3.2.17. *The above lemma tells us that $W(\theta, \psi) = (-1)^{n(\psi)} W(\chi \otimes \gamma, \psi \circ \mathrm{Tr}_{L^H/K})$ whenever θ is self-dual.*

All that remains is to compute $W(\chi \otimes \gamma, \psi \circ \mathrm{Tr}_{L^H/K})$, for which we use the theorem of Fröhlich and Queyrut [FQ73, p.130].

Theorem 3.2.18 (Fröhlich–Queyrut)**.** *Let K_1 be a local field, K_2 a quadratic extension of K_1. Let $u \in K_2$ be such that $K_2 = K_1(u)$ and $u^2 \in K_1$. Then if λ is a character of $K_2^\times$ which is trivial on $K_1^\times$, then $W(\lambda, \psi_2) = \lambda(u)$ for any non-trivial additive character ψ_2 of K_2.*

Remark 3.2.19. *Note that if K_2/K_1 is unramified, then we may assume that $u \in \mathcal{O}_{K_2}^\times$ so any unramified characters will act trivially on u.*

Observe that $\chi \otimes \gamma$ is a character of $(L^H)^\times$, the fixed field of H; to apply this theorem we examine $(\chi \otimes \gamma)|_{(L^{H'})^\times}$, where $L^{H'}$ is fixed field of $H' = \langle \iota, \mathrm{Frob}^{f/2} \rangle$ and is the unique quadratic subfield of L^H containing K.

Let $\mu = \mathrm{Ind}_H^{H'} \chi \otimes \gamma$. By the determinant formula [Gal65, (1)], we observe that $\det \mu = \mathrm{sign}_{[H':H]} \otimes (\chi \otimes \gamma)|_{(L^{H'})^\times}$ so we only need to compute $\det \mu$. Choosing representatives $\{1, \mathrm{Frob}^{f/2}\}$ for H'/H, we find that

$$\mu(\iota) = \begin{pmatrix} \chi(\iota) & 0 \\ 0 & \chi(\iota^{-1}) \end{pmatrix}, \qquad \mu(\mathrm{Frob}^{f/2}) = \begin{pmatrix} 0 & \gamma(\mathrm{Frob}^f) \\ 1 & 0 \end{pmatrix},$$

where we have used that $q^{f/2} \equiv -1 \bmod e$ since θ is self-dual (cf. Lemma 3.2.3iv). We find that $\det \mu = \begin{cases} \mathbb{1}_{H'} & \text{if } \theta \text{ is symplectic,} \\ \mathrm{sign}_{[H':H]} & \text{if } \theta \text{ is orthogonal.} \end{cases}$

Lemma 3.2.20. *Let θ be an irreducible, self-dual, tamely ramified Weil representation with $\theta = \mathrm{Ind}\, \chi \otimes \gamma$ as in Lemma 3.2.3.*

i. If θ is symplectic, then $W(\theta, \psi) = -\chi(u)$.

ii. If θ is orthogonal, then $W(\theta, \psi) = (-1)^{n(\psi)}\chi(u)$.

Proof. (i): First suppose that θ is symplectic, so γ is a non-trivial quadratic character. Then $(\chi \otimes \gamma)|_{(L^{H'})^\times} = \mathrm{sign}_{[H':H]}$ and hence $(\chi \otimes \gamma \otimes \mathrm{sign}_{[H':H]})|_{(L^{H'})^\times}$ is trivial. Now by the theorem of Fröhlich and Queyrut and Remark 3.2.19,

$$W(\chi \otimes \gamma \otimes \mathrm{sign}_{[H':H]}, \psi \circ \mathrm{Tr}_{L^H/K}) = (\chi \otimes \gamma \otimes \mathrm{sign}_{[H':H]})(u) = \chi(u).$$

On the other hand,

$$\begin{aligned} W(\chi \otimes \gamma \otimes \mathrm{sign}_{[H':H]}, \psi \circ \mathrm{Tr}_{L^H/K}) &= W(\chi \otimes \gamma, \psi \circ \mathrm{Tr}_{L^H/K})\, \mathrm{sign}_{[H':H]}(\mathrm{Frob}^{f/2})^{n(\psi)+1} \\ &= (-1)^{n(\psi)+1}\chi(u). \end{aligned}$$

By Remark 3.2.17, we hence have $W(\theta, \psi) = (-1)^{2n(\psi)+1}\chi(u)$ which proves our result.

(ii): Now suppose that θ is orthogonal. Then $(\chi \otimes \gamma)|_{(L^{H'})^\times}$ is already trivial so we are in a position to apply the theorem of Fröhlich and Queyrut directly; proceeding as above we find the stated root number formula. □

Remark 3.2.21. *Despite appearances, we have now shown the independence of the root number of B/K, an abelian variety with potentially good reduction, on the choice of additive character ψ whenever B/K has tame reduction. A priori, the only case we should concern ourselves with is when the self-dual summands are orthogonal.*

However, since $\rho_B \otimes \chi_{cyc}^{1/2}$ is symplectic, it must contain an even number of orthogonal summands [Sab07, Lemma A.2] so the overall root number of B/K is indeed independent. For computational reasons, we shall henceforth assume that $W(\theta, \psi) = -\chi(u)$ as this will not affect $W(\rho_B, \psi)$ and omit ψ from our notation.

Finally we derive criteria for determining $\chi(u)$, where $L^H = L^{H'}(u)$ with $u^2 \in L^{H'}$ and recall that we may suppose $u \in \mathcal{O}_{L^H}^\times$ by Remark 3.2.19.

Lemma 3.2.22. *Let $k_H, k_{H'}$ be the residue fields of the fixed fields L^H and $L^{H'}$ respectively and let $\tilde{q} = |k_{H'}|$. Let χ be a tamely ramified which satisfies the conditions of Theorem 3.2.18 with respect to the extension $L^H/L^{H'}$. Suppose χ has order e on $\mathcal{O}_{L^H}^\times$. If $\tilde{q}$ is even, then $\chi(u) = 1$. Otherwise*

$$\chi(u) = 1 \Leftrightarrow v_2(\tilde{q}+1) \geqslant v_2(e) + 1,$$

where v_2 is the 2-adic valuation.

Proof. If $\tilde{q}$ is even, then e is odd and hence $\chi(u) = 1$ (cf. proof of Lemma 3.2.8), so we now suppose $\tilde{q}$ is odd. If e is not a power of 2, then we may write $\chi = \chi_1 \otimes \chi_2$, where χ_1 has odd order and the order of χ_2 is a power of 2 on $\mathcal{O}_{L^H}^\times$. Then, as before, $\chi_1(u) = 1$ and hence we may suppose that $\chi = \chi_2$. As χ is tamely ramified, it is trivial on principal units and hence we shall view its action on the quotient instead and identify u, u^2 with their images after an isomorphism to $k_H^\times$ and $k_{H'}^\times$.

Now note $k_{H'} \cong \mathbb{F}_{\tilde{q}}$, $k_{L^H} \cong \mathbb{F}_{\tilde{q}^2}$ as $L^H/L^{H'}$ is unramified. Let $k_H^\times = \langle \xi \rangle$ and observe that $k_{H'}^\times = \langle \xi^{\tilde{q}+1} \rangle$. Let $u = \xi^a$. As $u^2 \in k_{H'}$, $(\tilde{q}+1)|2a$ and moreover $(\tilde{q}+1) \nmid a$ since $u \notin k_{H'}$. Therefore $v_2(\tilde{q}+1) = v_2(2a) = v_2(a) + 1$.

As χ has order e, we have

$$\begin{aligned}
\chi(u) = 1 &\Leftrightarrow u \in \left(k_H^\times\right)^e, \\
&\Leftrightarrow e|a, \\
&\Leftrightarrow v_2(e) \leqslant v_2(a), \\
&\Leftrightarrow v_2(e) \leqslant v_2(\tilde{q}+1) - 1,
\end{aligned}$$

where the penultimate equivalence follows from our earlier reduction of supposing e has 2-power order. □

Remark 3.2.23. *We used $\tilde{q}$ for the size of the residue field to remind the reader that this need not be equal to q since we have had to move to an intermediate field. In fact, if θ is f-dimensional, then $\tilde{q} = q^{f/2}$.*

We now combine the previous two lemmas to give a complete description of $W(\theta)$ where we intentionally fail to distinguish between the orthogonal and symplectic cases (cf. Remark 3.2.21).

Theorem 3.2.24. *Let θ be an irreducible, self-dual, tamely ramified Weil representa-*

tion of dimension $f \geqslant 2$ such that $|\theta(I)| = e$. If q is even, then $W(\theta) = -1$. Otherwise

$$W(\theta) = 1 \Leftrightarrow v_2(q^{f/2} + 1) = v_2(e).$$

Proof. Recall $W(\theta) = -\chi(u)$. If q is even, the result follows immediately. When q is odd, observe that $-\chi(u) = 1$ if and only if $v_2(q^{f/2} + 1) < v_2(e) + 1$ if and only if $v_2(q^{f/2} + 1) \leqslant v_2(e)$. Since the representation is self-dual, we have that $q^{f/2} \equiv -1 \bmod e$ and hence we always have $v_2(q^{f/2} + 1) \geqslant v_2(e)$. □

Remark 3.2.25. *Note that if e is odd then $W(\theta) = -1$ regardless of whether q is odd or even. Combining this with Remark 3.2.12, we do not need to distinguish between q being odd or even in the potentially good reduction situation.*

3.2.4 Packaging the representation

So far we have concentrated on the irreducible summands but we now collate such summands to connect the root numbers of particular types of representations to certain Jacobi symbols depending on e.

Lemma–Definition 3.2.26. *Let ρ be a symplectic, tamely ramified Weil representation such that the characteristic polynomial of $\rho(\iota)$ has coefficients in $\mathbb{Z}$. Let ρ_1 be an irreducible summand of ρ such that $|\rho_1(I)| = e$. Then there exists irreducible summands $\rho_2, \cdots, \rho_m$ of ρ such that:*

i. $\dim \rho_1 = \cdots = \dim \rho_m$,

ii. $m \dim \rho_1 = \tilde{\varphi}(e)$,

iii. Consider the $\tilde{\varphi}(e)$ eigenvalues of $\rho_j(\iota)$, $j = 1, \cdots, m$.

   (a) If $e \leqslant 2$, then there is only one eigenvalue (with multiplicity 2).

   (b) If $e \geqslant 3$, then all eigenvalues are distinct.

We define ρ_e to be any representation of the form $\bigoplus_{j=1}^{m} \rho_j$. Moreover, ρ can be decomposed into summands of the form ρ_e.

Proof. Observe that since ρ_1 is irreducible, all eigenvalues are primitive e-th roots unity (cf. proof of Lemma 3.2.1). Since the characteristic polynomial of $\rho(\iota)$ has coefficients in $\mathbb{Z}$, there are necessarily irreducible summands $\rho_2, \cdots, \rho_{m'}$ such that the characteristic polynomial of $\bigoplus_{j=1}^{m'} \rho_j(\iota)$ is the e-th cyclotomic polynomial.

If $e \leqslant 2$, then $m' = 1$ and $\dim \rho_1 = 1$ but we are done by applying Lemma 3.2.4 (hence $m = 2$), so we may now assume $e \geqslant 3$. In this case we have all $\tilde{\varphi}(e)$ eigenvalues and they are distinct since the cyclotomic polynomial is separable so $m' = m$. To see that the summands have equal dimension, note that this is controlled by the order of $q \bmod e$ due to the relation $\mathrm{Frob}\, \iota\, \mathrm{Frob}^{-1} = \iota^q$; indeed the sets of eigenvalues of the $\rho_j(\iota)$ correspond to cosets of the subgroup $\langle q \rangle \subset (\mathbb{Z}/e\mathbb{Z})^\times$.

To see that ρ has a decomposition into summands of this form, note that the rationality of the characteristic polynomial forces the correct multiplicities for $e \geqslant 3$ and the symplectic condition does the same for $e = 1, 2$ by Lemma 3.2.4. □

For the rest of this section, we wish to suppose that our representations ρ_e are themselves symplectic to apply our results compute their corresponding root numbers. Our first step in this direction to is to prove that they are self-dual, after possibly reordering the summands.

Lemma 3.2.27. *Let ρ be a symplectic, tamely ramified Weil representation such that the characteristic polynomial of $\rho(\iota)$ has coefficients in $\mathbb{Z}$. Then there exists a decomposition of $\rho = \bigoplus \rho_{e_j}$ such that each ρ_{e_j} is self-dual and satisfies Definition 3.2.26.*

Proof. Let $\rho = \bigoplus_{j=1}^{k} \rho_{e_j}$ be a decomposition into summands satisfying Definition 3.2.26. If all summands ρ_{e_j} are self-dual then we are done.

Otherwise, there exists j and some irreducible summand σ of ρ_{e_j} such that σ^* is not a subrepresentation of ρ_{e_j}. Since ρ is self-dual, there exists $j' \neq j$ such that σ^* is a subrepresentation of $\rho_{e_{j'}}$ and moreover as $|\sigma(I)| = |\sigma^*(I)|$, $e_j = e_{j'}$, i.e. their eigenvalues on ι have the same order.

If $e_j \geqslant 3$, then note that as σ is not self-dual, $\sigma^*(\iota)$ has distinct eigenvalues to $\sigma(\iota)$ and hence we may replace the corresponding summand of ρ_{e_j} with σ^* and still obtain a representation satisfying Definition 3.2.26. Note that the summand we have replaced did not have its dual as a subrepresentation of ρ_e since this would have necessarily have been σ itself. Therefore we can iterate this process and it will eventually terminate. If $e_j < 3$, then there is only one eigenvalue and we replace the only other summand with σ^* from which the same argument then applies. □

We briefly state the classical push-pull formula for representations without proof, which we shall use momentarily.

Lemma 3.2.28 (Push-pull formula)**.** *Let G be a group, H a subgroup of finite index in G. Let ρ_H, ρ_G be finite dimensional complex representations of H and G respectively. Then*

$$(\mathrm{Ind}_H^G \rho_H) \otimes \rho_G \cong \mathrm{Ind}_H^G(\rho_H \otimes \mathrm{Res}_H^G \rho_G).$$

Lemma 3.2.29. *Let θ be an irreducible, self-dual, tamely ramified Artin representation of $\mathrm{Gal}(\overline{K}/K)$ with $\dim\theta \geqslant 2$ and let ν be any unramified character of order $2\dim\theta$. If θ is orthogonal (resp. symplectic), then $\theta \otimes \nu$ is symplectic (resp. orthogonal) and moreover $W(\theta \otimes \nu) = -W(\theta)$.*

Proof. Let $f = \dim\theta$, $e = |\theta(I)| > 1$. Then by Lemma 3.2.3, θ factors through a Galois extension L/K where $\mathrm{Gal}(L/K) = \langle \iota, \mathrm{Frob}\,|\iota^e, \mathrm{Frob}^{2f}, \mathrm{Frob}\,\iota\,\mathrm{Frob}^{-1} = \iota^q\rangle$, and $q^f \equiv 1 \bmod e$. Now let ν' be any unramified character for $\mathrm{Gal}(L/K)$. Recall that $\theta = \mathrm{Ind}_{L^H/K}\chi \otimes \gamma$ is monomial and hence by the push-pull formula (Lemma 3.2.28), we have

$$\begin{aligned} \theta \otimes \nu' &= (\mathrm{Ind}_{L^H/K}\chi \otimes \gamma) \otimes \nu', \\ &= \mathrm{Ind}_{L^H/K}(\chi \otimes \gamma \otimes \mathrm{Res}_{L^H/K}\nu'). \end{aligned}$$

Let ν be a primitive unramified character of $\mathrm{Gal}(L/K)$ so ν has order $2f$ and note that $\mathrm{Res}_{L^H/K}\nu^r = \mathbb{1}$ if and only if r is even. Moreover, as ν is primitive, $\theta \otimes \nu \ncong \theta$ since $(\theta\otimes\nu)(\mathrm{Frob}^f) = (\gamma\otimes\nu)^{\oplus f}(\mathrm{Frob}^f) = -\gamma(\mathrm{Frob}^f)^{\oplus f} \ncong \gamma(\mathrm{Frob}^f)^{\oplus f}$.

We distinguish between orthogonal and symplectic representations via the Frobenius–Schur indicator: if π is an irreducible self-dual representation of a finite group G then $S(\pi) := \frac{1}{|G|}\sum_{g\in G}\mathrm{Tr}\,\pi(g^2)$ is such that $S(\pi) = 1$ if π is orthogonal and $S(\pi) = -1$ if π is symplectic. We show that $S((\theta\otimes\nu)\oplus\theta) = 0$ from which the result follows since $S(\pi_1\oplus\pi_2) = S(\pi_1) + S(\pi_2)$ for any representations π_1, π_2.

In fact, we note that since $\theta\otimes\nu^r$ only depends on the parity of r, we have that

$$fS((\theta\otimes\nu)\oplus\theta) = S\left(\theta \otimes \left(\bigoplus_{r=1}^{2f}\nu^r\right)\right),$$

so we work with the right hand side since $\bigoplus_{r=1}^{2f}\nu^r = \theta_{reg}$ is the inflation of the regular representation on $\mathrm{Gal}(L^I/K)$.

Now $\operatorname{Tr}\theta_{reg}(\operatorname{Frob}^k \iota^l) = \operatorname{Tr}\theta_{reg}(\operatorname{Frob}^k) = 0$ unless $k = 0$. Hence for $k \neq 0$,

$$\operatorname{Tr}(\theta \otimes \theta_{reg})(\operatorname{Frob}^k \iota^l) = (\operatorname{Tr}\theta(\operatorname{Frob}^k \iota^l)) \cdot (\operatorname{Tr}\theta_{reg}(\operatorname{Frob}^k \iota^l)) = 0.$$

Using the group structure, we note that $(\operatorname{Frob}^k \iota^l)^2 = \operatorname{Frob}^{2k} \iota^{l_1}$ for some l_1, and therefore the only terms that contribute are in the abelian subgroup $\langle \operatorname{Frob}^f, \iota \rangle$, where θ_{reg} acts as the identity.

We now compute

$$\begin{aligned} \frac{|\operatorname{Gal}(L/K)|}{\dim \theta_{reg}} S(\theta \otimes \theta_{reg}) &= \sum_{k=0}^{1} \sum_{l=1}^{e} \operatorname{Tr}\theta((\operatorname{Frob}^{kf} \iota^l)^2), \\ &= 2 \sum_{l=1}^{e} \operatorname{Tr}\theta(\iota^{2l}). \end{aligned}$$

Since θ is tamely ramified, we may suppose it acts diagonally on ι. Let ζ_e be an eigenvalue of $\theta(\iota)$ so the corresponding eigenvalues of $\theta(\iota^l)$ are ζ_e^l.

If e is odd, then $2l$ runs through all possible powers of ζ_e and we are done since $\sum_{l=1}^{e} \zeta_e^l = 0$ is the trace of $x^e - 1$. If e is even, then we instead get twice the trace of $x^{e/2} - 1$ and are again done.

Finally observe that by Theorem 2.2.1iii,

$$W(\theta \otimes \nu) = W(\theta)\nu(\operatorname{Frob})^{a(\theta)} = W(\theta)\nu(\operatorname{Frob})^{\dim \theta} = -W(\theta)$$

since ν is an unramified character of order $2 \dim \theta$. □

Before we prove that we may suppose that the ρ_e are symplectic, we need a lemma concerning the structure of semisimple symplectic representations.

Lemma 3.2.30. *Let ρ be a semisimple symplectic representation of a group G. Then there exists irreducible symplectic representations $\lambda_1, \cdots \lambda_t$ of G and a representation π of G such that*

$$\rho \cong \pi \oplus \pi^* \oplus \lambda_1 \oplus \cdots \oplus \lambda_t.$$

Proof. See [Sab07, Lemma A.2]. □

Remark 3.2.31. *Unfortunately, we cannot simply reorganise the summands between the different ρ_e to show they are symplectic; indeed suppose ρ_e is self-dual but not*

symplectic and consider the symplectic representation $\rho = \rho_e^{\oplus 2}$. This does not have a symplectic decomposition as desired due to our assumption of ρ_e on inertia.

We are finally in a position to show that the ρ_e may be assumed to be symplectic, without affecting the overall root number of the overarching symplectic representation.

Theorem 3.2.32. *Let ρ_e be a Weil representation as in Definition 3.2.26. Write*

$$\rho_e \cong \pi \oplus \pi^* \oplus \bigoplus_{j=1}^{m} \theta_j,$$

such that θ_j are irreducible self-dual summands. Let

$$\rho'_e = \pi \oplus \pi^* \oplus \bigoplus_{j=1}^{m} \theta_j \otimes \nu_j,$$

where ν_j are unramified characters of finite order such that $\theta_j \otimes \nu_j$ is symplectic for all j. Then ρ'_e satisfies Definition 3.2.26 and $W(\rho'_e) = (-1)^a W(\rho_e)$, where a is the number of summands θ_j which are orthogonal.

Moreover, if ρ is a symplectic tamely ramified Weil representation such that we have a decomposition $\rho \cong \bigoplus \rho_{e_j}$ into summands satisfying Definition 3.2.26, then $W(\rho) = \prod W(\rho'_{e_j})$.

Proof. First note that ρ'_e satisfies Definition 3.2.26 since it only specifies the action on inertia. To see that it is symplectic, observe that a sum of symplectic representations is symplectic and if V is a vector space with dual space V^*, then we can define a symplectic form on $V \oplus V^*$ by

$$((v_1, A_1), (v_2, A_2)) \mapsto A_2(v_1) - A_1(v_2).$$

The fact that $W(\rho'_e) = (-1)^a W(\rho_e)$ follows directly from Lemma 3.2.29. Finally, note that since ρ is symplectic, the number of irreducible orthogonal summands of ρ must be even from Lemma 3.2.30 and the result follows. □

Remark 3.2.33. *If B/K is an abelian variety with potentially good reduction, then $\rho_B \otimes \chi_{cyc}^{1/2}$ satisfies the conditions of Definition 3.2.26, hence $\rho_B \otimes \chi_{cyc}^{1/2}$ decomposes into self-dual summands ρ_{e_j} (cf. Definition 3.2.26). By Corollary 2.2.6 and Theorem*

3.2.32, we therefore have

$$W(\rho_B) = W(\rho_B \otimes \chi_{cyc}^{1/2}) = \prod_{j=1}^{k} W(\rho'_{e_j}),$$

where ρ'_{e_j} is the symplectic version of ρ_{e_j} as in Theorem 3.2.32. All that remains is to explicitly describe $W(\rho_{e_j})$ when ρ_{e_j} is symplectic.

3.2.5 Jacobi symbols

With a symplectic representation ρ_e (cf. Definition 3.2.26) fixed, we shall allow q to vary and study the effect on the root number of ρ_e. Whilst our original results seemed dependent on the parity of q, this is in fact a red herring (cf. Remark 3.2.25) and so we shall not distinguish between the cases in the following proofs.

Note that since we have only assumed tame inertia, q is necessarily coprime to e hence it is reasonable to expect a Jacobi symbol connected to q and e. Our first step in this direction is the following lemma.

Lemma 3.2.34. *Let l be an odd prime and $e = l^k$. Then $W(\rho_e) = \left(\frac{q}{l}\right)$.*

Proof. Note that $(\mathbb{Z}/e\mathbb{Z})^\times$ is cyclic, so let ξ be a generator of this group and let n be such that $q \equiv \xi^n \bmod e$. Note that as the dimension of an irreducible summand is equal to the order of $q \bmod e$, the number of such summands is $\gcd(n, \tilde{\varphi}(e))$.

If n is odd, then we have an odd number of irreducible summands which are all necessarily self-dual (this depends only on q and e so they are either all dual or all self-dual) since dual summands arise in pairs. Now self-dual summands have a negative root number by Remark 3.2.25 and hence $W(\rho_e) = (-1)^{\gcd(n,\tilde{\varphi}(e))} = -1$.

If n is even, then $\gcd(n, \tilde{\varphi(e)})$ is even. If each summand is self-dual, then we have $W(\rho_e) = (-1)^{\gcd(n,\tilde{\varphi}(e))} = 1$. On the other hand, if the summands arise in dual pairs then $W(\rho_e) = 1^{\gcd(n,\tilde{\varphi}(e))/2} = 1$ by Remark 3.2.12. □

We now consider the case $l = 2$ to obtain a similar result. We note that cases $e = 2, 4$ have been covered by Rohrlich; since these give separate Legendre symbols, we omit those cases here.

Lemma 3.2.35. *Let $e = 2^n$ for $n \geqslant 3$. Then $W(\rho_e) = -1$ if and only if the irreducible summands arise in dual pairs and $q \bmod e$ has order 2^{n-2}.*

Proof. By our hypotheses, $(\mathbb{Z}/e\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$. Since -1 is not a square in $\mathbb{Z}_2$, it cannot be a square modulo e, so the only self-dual case that occurs is when $q \equiv -1 \bmod e$. In this case, the irreducible summands are 2-dimensional and hence there are 2^{n-2} such summands. As $n \geqslant 3$, this is even and hence $W(\rho_e) = 1$.

We are now reduced to considering dual pairs. Let an irreducible summand have dimension f which divides 2^{n-2}. If f is not maximal, then we have an even number of dual pairs and hence $W(\rho_e) = 1$. All that remains to deal with is the case $f = 2^{n-2}$.

Using the group structure, there are 3 non-trivial square roots of 1 and since the irreducible summands are not self-dual, we necessarily have $q^{f/2} \equiv 2^{n-1} \pm 1 \bmod 2^n$. Writing $q^{f/2} = 2^n \pm 1 + 2^n k$, we compute that

$$q^f = 1 \pm 2^n \pm 2^{n+1}k + 2^{2n-2} + 2^{2n}k(1+k),$$

from which we observe that $v_2(q^f - 1) = n$.

Now

$$\begin{aligned} v_2\left(\gcd\left(2^n, \frac{q^f-1}{q-1}\right)\right) &= \min\left(v_2(2^n), v_2\left(\frac{q^f-1}{q-1}\right)\right), \\ &= \min(n, v_2(q^f-1) - v_2(q-1)), \\ &= \min(n, n - v_2(q-1)), \\ &= n - v_2(q-1). \end{aligned}$$

The congruence we obtain from Lemma 3.2.9 is therefore $q \equiv 1 \bmod 2^{v_2(q-1)}$, and hence will always yield a negative root number. □

Since we would like our root number to be phrased in terms of a Legendre symbol, we shall now characterise the primes p which have maximal order.

Lemma 3.2.36. *Let q be a power of an odd prime and $e = 2^n$. Then $W(\rho_e) = \left(\frac{2}{q}\right)$.*

Proof. Observe that $\left(\frac{2}{q}\right) = -1$ if and only if $q \equiv 3, 5 \bmod 8$. We first show that any prime of this form has maximal order, so let $q \equiv 3, 5 \bmod 8$ and note that these are exactly by characterised by $v_2(q^2 - 1) = 3$, where v_2 is the 2-adic valuation. More generally, we claim that $v_2(q^{2^{n-2}} - 1) = n$ for $n \geqslant 3$ by induction, using $n = 3$ as our base case.

To prove the inductive step, suppose $v_2(q^{2^{k-2}} - 1) = k$ and write $q^{2^{k-2}} = 1 + u2^k$ for

some odd integer u. Then $q^{2^{k-1}} = (1+u2^k)^2 = 1+u2^{k+1}+u^2 2^{2k}$ and hence the claim follows as u is odd and $k \geqslant 3$. Now if $q \bmod e$ did not have order 2^{n-2}, then $q^{2^{n-3}} \equiv 1 \bmod e$ and hence $v_2(q^{2^{n-3}}-1) \geqslant n$ which contradicts our claim.

Conversely, let $q \equiv 1, 7 \bmod 8$. If $n = 3$, then we can check this case directly where we note that although 7 has maximal order, this happens to correspond to the self-dual case and therefore will have positive root number. We now claim that $v_2(q^{2^{n-3}}-1) \geqslant n$ for $n \geqslant 4$.

The base case is again verified directly and for the inductive step, we proceed similarly by noting that if $q^{2^{k-3}} = 1+u2^k$ for some integer u, then $q^{2^{k-2}} = 1+u2^{k+1}+u^2 2^{2k}$ from which the claim follows. □

The general idea is that the group of units should be cyclic (with the exception where e is power of 2; a case which we shall now forget about since we have dealt with it). We shall now prove this statement.

Lemma 3.2.37. *Let e be an integer which is neither a prime power nor twice a prime power. Then $W(\rho_e) = 1$ independently of q.*

Proof. Observe that $(\mathbb{Z}/2\mathbb{Z})^2 \leqslant (\mathbb{Z}/e\mathbb{Z})^\times$ and therefore any cyclic subgroup of $(\mathbb{Z}/e\mathbb{Z})^\times$ has even index. First suppose that the irreducible summands are self-dual. Then since the image of inertia of a summand is cyclic, there is an even number of such summands and therefore $W(\rho_e) = 1$. Hence we may suppose that such a summand is part of a dual pair.

Note that the image of inertia of a dual pair has order twice the size of a cyclic subgroup, hence if $(\mathbb{Z}/2\mathbb{Z})^3 \leqslant (\mathbb{Z}/e\mathbb{Z})^\times$ then we have an even number of dual pairs so $W(\rho_e) = 1$ again. This reduces us to checking the case $e = 4l^k$ where l is an odd prime. Let f be the order of $q \bmod e$ and let v_2 denote the 2-adic valuation. As $(\mathbb{Z}/2\mathbb{Z})^2 \leqslant (\mathbb{Z}/e\mathbb{Z})^\times$, $v_2(f) < v_2(e) = 1 + v_2(l-1)$. If $v_2(f) \neq v_2(l-1)$, then similarly to before, we again must have an even number of dual pairs so are done.

We may now assume $v_2(f) = v_2(l-1) \geqslant 1$ and we claim that the root number of each

dual pair $\sigma \oplus \sigma^*$ is 1 which would complete the proof. By Theorem 3.2.10, we have:

$$\begin{aligned} W(\sigma \oplus \sigma^*) = 1 \Leftrightarrow \quad & q \equiv 1 \bmod \frac{2e}{\gcd(e, \frac{q^f-1}{q-1})}, \\ \Leftrightarrow \quad & q \equiv 1 \bmod \frac{2e}{\gcd(e, q^{f-1}+q^{f-2}+\cdots+1)}, \\ \Leftrightarrow \quad & v_2(q-1) \geqslant v_2\left(\frac{2e}{\gcd(e, q^{f-1}+q^{f-2}+\cdots+1)}\right) \text{ by Lemma 3.2.9,} \\ \Leftrightarrow \quad & v_2(q-1) \geqslant 3 - \min\{2, v_2(q^{f-1}+q^{f-2}+\cdots+1)\}. \end{aligned}$$

Note that there are f terms in $q^{f-1}+q^{f-2}+\cdots+1$ so $v_2(q^{f-1}+q^{f-2}+\cdots+1) \geqslant 1$ as $v_2(f) \geqslant 1$. If $q \equiv 1 \bmod 4$ then we are done so suppose $q \equiv 3 \bmod 4$. In this case, we have

$$\begin{aligned} q^{f-1}+q^{f-2}+\cdots+1 \quad & \equiv \quad (-1)^{f-1}+(-1)^{f-2}+\cdots+1 \bmod 4, \\ & \equiv \quad 0 \bmod 4, \end{aligned}$$

so $\min\{2, v_2(q^{f-1}+q^{f-2}+\cdots+1)\} = 2$ which proves the claim. □

This shows that in order to obtain a negative root number, the unit group should be cyclic. However, this is not quite sufficient as we shall now demonstrate.

Lemma 3.2.38. *Let l be an odd prime such that $l \equiv 1 \bmod 4$ and let $e = 2l^k$. Then $W(\rho_e) = 1$ for all q.*

Proof. Since $l \equiv 1 \bmod 4$, -1 is a square modulo e since the unit group is cyclic. If f is the order of $q \bmod e$, then an irreducible summand is self-dual if and only if f is even; indeed in this case $q^{f/2} \equiv -1 \bmod e$. If the summand is not self-dual, then since there are $\dfrac{\tilde{\varphi}(e)}{f}$ summands we have an even number of dual pairs which implies that $W(\rho_e) = 1$.

Similarly, if $v_2(f) \neq v_2(\tilde{\varphi}(e))$, then we have an even number of irreducible self-dual summands are again done. So assume $v_2(f) = v_2(\tilde{\varphi}(e))$ which implies that $4|f$. The criterion in Theorem 3.2.24 states that we have a positive root number if and only if $v_2(q^{f/2}+1) = 1$. This holds since the only square in $(\mathbb{Z}/4\mathbb{Z})^\times$ is 1; i.e. if $f = 4k$, then as q is odd, $q^{f/2} = q^{2k} \equiv 1 \bmod 4$. □

We only have one more case left to study before collating these results into a theorem.

Lemma 3.2.39. *Let l be an odd prime such that $l \equiv 3 \bmod 4$ and let $e = 2l^k$. Then* $W(\rho_e) = \left(\frac{-1}{q}\right)$.

Proof. Let f be the order of $q \bmod e$. Similarly to the above proof, we have that an irreducible summand is self-dual if and only if f is even. This implies we either have an odd number of dual pairs or an odd number of self-dual summands and hence $W(\rho_e)$ is the same as the root number of a dual pair or irreducible self-dual summand.

First suppose f is odd so we are in the dual case. We claim that $v_2(q-1) = v_2(q^f-1)$. Indeed, let n be such that $v_2(q-1) = n$ so $q \equiv 1 + 2^n \bmod 2^{n+1}$. Then

$$\begin{aligned} q^f &\equiv (1+2^n)^f \bmod 2^{n+1}, \\ &= \sum_{j=0}^{f} \binom{f}{j} 2^{nj}, \\ &= 1 + f2^n + 2^{2n} \sum_{j=2}^{f} \binom{f}{j} 2^{nj}, \\ &\equiv 1 + 2^n \bmod 2^{n+1} \end{aligned}$$

which proves the claim.

Similarly to the proof of Lemma 3.2.37:

$$\begin{aligned} W(\rho_e) = 1 &\Leftrightarrow q \equiv 1 \bmod \frac{2e}{\gcd(e, \frac{q^f-1}{q-1})}, \\ &\Leftrightarrow v_2(q-1) \geqslant v_2(2e) - \min\{v_2(e), v_2(q^f-1) - v_2(q-1)\}, \\ &\Leftrightarrow v_2(q-1) \geqslant 2. \end{aligned}$$

Now assume the irreducible summands are self-dual so f is even and moreover $f \equiv 2 \bmod 4$. Here we claim that $v_2(q^{f/2}+1) = v_2(q+1)$. In fact if $v_2(q+1) = n$ then $q \equiv -1 + 2^n \bmod 2^{n+1}$ and we similarly have

$$\begin{aligned} q^{f/2} &\equiv (-1+2^n)^{f/2} \bmod 2^{n+1}, \\ &= \sum_{j=0}^{f/2} \binom{f/2}{j} (-1)^{\frac{f}{2}-j} 2^{nj}, \\ &\equiv -1 + \frac{f}{2} 2^n \bmod 2^{n+1} \qquad \text{as } f \equiv 2 \bmod 4, \\ &\equiv -1 + 2^n \bmod 2^{n+1}. \end{aligned}$$

Hence by Theorem 3.2.24, $W(\rho_e) = 1 \Leftrightarrow v_2(q+1) = 1$ and the stated Jacobi symbol follows. □

We now collate this section into a single theorem.

Theorem 3.2.40. *Let ρ_e be a symplectic representation satisfying Definition 3.2.26 and let q be the cardinality of the residue field of K. Then*

$$W(\rho_e) = \begin{cases} \left(\frac{q}{l}\right) & \text{if } e = l^k; \\ \left(\frac{-1}{q}\right) & \text{if } e = 2l^k \text{ and } l \equiv 3 \bmod 4 \qquad \text{or } e = 2; \\ \left(\frac{-2}{q}\right) & \text{if } e = 4; \\ \left(\frac{2}{q}\right) & \text{if } e = 2^k \text{ for } k \geqslant 3; \\ 1 & \text{else,} \end{cases}$$

for any integer $k > 0$ and rational prime $l \geqslant 3$.

Remark 3.2.41. *Note that if q is a square, then $W(\rho_e) = 1$.*

3.3 Potentially totally toric reduction

We now compute the root number $W(\rho_T \otimes \chi_{cyc} \otimes \mathrm{sp}(2), \psi) = W(\rho_T \otimes \mathrm{sp}(2), \psi)$. Recall that ρ_T is defined over $\mathbb{Z}$ by Fact 2.3.2, so in particular has real character.

Lemma 3.3.1. *[Roh96, p.14] Let τ be an Artin representation of $\mathrm{Gal}(\overline{K}/K)$ with real character. Then*

$$W(\tau \otimes \mathrm{sp}(2), \psi) = (-1)^{\langle \mathbb{1}, \tau \rangle}((\det \tau)(-1)).$$

Remark 3.3.2. *As we have now covered all cases, we can see that we have now completely proven the independence of the root number on ψ for any symplectic Weil representation (and hence also for any abelian variety A/K) which is tamely ramified. We shall therefore now omit this notation from here on.*

When ρ_T is tamely ramified, we use Theorem 3.2.10 where $f = \dim \rho_T$, which only requires knowledge of the action of inertia on ρ_T. We do however need to know the multiplicity of $\mathbb{1}$ hence we also need some information about the action of ρ_T on Frobenius. To this end, we use the Euler factor and compute the multiplicity of $x - 1$ of the

local polynomial.

So far we have not used the assumption that ρ_T is tamely ramified in this section; indeed Rohrlich gives an explicit formula at $p = 3$. We shall do similarly under some constraints to make the result of Lemma 3.3.1 more explicit.

Lemma 3.3.3. *Assume that $\rho_T(I)$ is abelian and $p > 2$. Let χ_1, χ_2 be the ramified quadratic characters of K. Then* $(\det \rho_T)(-1) = \left(\frac{-1}{q}\right)^{\langle \rho_T, \chi_1 \oplus \chi_2 \rangle}$.

Theorem 3.3.4. *Suppose ρ_T is tamely ramified and let m_T be the multiplicity of -1 as an eigenvalue of $\rho_T(\iota)$. Then*

$$W(\rho_T \otimes \mathrm{sp}(2)) = (-1)^{\langle \mathbb{1}, \rho_T \rangle} \left(\frac{-1}{q}\right)^{m_T}.$$

Combining this with Theorem 3.2.40, we have now proved our first main result.

Theorem 3.3.5. *Let A/K be an abelian variety over a non-Archimedean local field which has tame reduction. Then*

$$W(A/K) = \left(\prod_{e \in \mathbb{N}} W_{q,e}^{m_e}\right) (-1)^{\langle \mathbb{1}, \rho_T \rangle} W_{q,2}^{m_T},$$

where for an integer $k > 0$ and rational odd prime l:

$$W_{q,e} = \begin{cases} \left(\frac{q}{l}\right) & \text{if } e = l^k; \\ \left(\frac{-1}{q}\right) & \text{if } e = 2l^k \quad \text{and } l \equiv 3 \bmod 4 \qquad \text{or } e = 2; \\ \left(\frac{-2}{q}\right) & \text{if } e = 4; \\ \left(\frac{2}{q}\right) & \text{if } e = 2^k \quad \text{for } k \geqslant 3; \\ 1 & \text{else.} \end{cases}$$

3.4 Examples

We now use the results of Dokchitser, Dokchitser, Maistret and Morgan [DDMM] to obtain the information we need from the Jacobian of a genus two hyperelliptic curve (via a Weierstrass model) to compute the root number under our assumptions. We first

give the relevant definitions (see for example [AD17, §2.1]).

Definition 3.4.1. *Let $K/\mathbb{Q}_p$ be a finite extension and let $f \in \mathcal{O}_K[x]$ be a squarefree monic polynomial with set of roots R. Then a cluster $\mathfrak{s} \subset R$ is a nonempty set of roots of the form $R \cap \mathcal{D}$ where $\mathcal{D} \subset \overline{K}$ is a p-adic disc.*

To compute the root number, we also need some more notation to construct the relevant representations. We choose the normalised valuation on v of K and extend it to $\overline{K}$.

Notation. *We use the direct minus sign, $\ominus$, to denote the inverse operation of the direct sum $\oplus$ for representations, taken inside the Grothendieck group of virtual representations if necessary.*

Definition 3.4.2. *For a cluster $\mathfrak{s}$ of cardinality at least 2, we define:*

$d_\mathfrak{s}$ $= \min\{v(r-r') \mid r, r' \in \mathfrak{s}\}$, *called the depth of $\mathfrak{s}$;*

$\mathfrak{s}^0$ *the set of maximal subclusters of $\mathfrak{s}$ of odd cardinality;*

$I_\mathfrak{s}$ $= \mathrm{Stab}_I(\mathfrak{s})$;

$\mu_\mathfrak{s}$ $= \sum_{r \in R \setminus \mathfrak{s}} v(r - r_0)$ *for any $r_0 \in \mathfrak{s}$;*

$\epsilon_\mathfrak{s}$ $=$
$\begin{cases} 0 \text{ -representation of } I_\mathfrak{s} \text{ if } |\mathfrak{s}| \text{ is odd}; \\ \mathbb{1} \text{ -representation of } I_\mathfrak{s} \text{ if } |\mathfrak{s}| \text{ is even and } \mathrm{ord}_2\, \mu_\mathfrak{s} \geqslant 1; \\ \text{order two character of } I_\mathfrak{s} \text{ if } |\mathfrak{s}| \text{ is even and } \mathrm{ord}_2\, \mu_\mathfrak{s} < 1; \end{cases}$

$\lambda_\mathfrak{s}$ $= \frac{1}{2}(\mu_\mathfrak{s} + d_\mathfrak{s}|\mathfrak{s}^0|)$;

$\gamma_\mathfrak{s}$ *any character of $I_\mathfrak{s}$ of order equal to the prime-to-p part of the denominator of $\lambda_\mathfrak{s}$ (with $\gamma_\mathfrak{s} = \mathbb{1}$ if $\lambda_\mathfrak{s} = 0$);*

$V_\mathfrak{s}$ $= \gamma_\mathfrak{s} \otimes (\mathbb{C}[\mathfrak{s}^0] \ominus \mathbb{1}) \ominus \epsilon_\mathfrak{s}$.

Theorem 3.4.3 ([DDMM])**.** *Let $\ell \neq p$ be prime. Let $C : y^2 = f(x)$ be a hyperelliptic curve over K, and assume that $p \neq 2$. Then*

$$H^1_{\acute{e}t}(C/\overline{K}, \mathbb{Q}_\ell) \otimes_{\mathbb{Q}_\ell} \mathbb{C} \cong H^1_{ab} \oplus (H^1_t \otimes \mathrm{sp}(2))$$

as complex I-representations, with

$$H^1_{ab} = \bigoplus_{X/I} \mathrm{Ind}_{I_\mathfrak{s}}^I V_\mathfrak{s}, \quad H^1_t = \bigoplus_{X/I} (\mathrm{Ind}_{I_\mathfrak{s}}^I \epsilon_\mathfrak{s}) \ominus \epsilon_R,$$

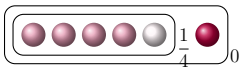
where X is the set of clusters that are not singletons and that cannot be written as a disjoint union of more than 2 clusters of even size.

Remark 3.4.4. *H^1_{ab} corresponds to the potentially good case whereas H^1_t corresponds*

to the potentially toroidal case. It is straightforward to see from the definition above that $\mathrm{Jac}(C)$ *has potentially good reduction if and only if all clusters except* R *have odd cardinality.*

Example 3.4.5. *Let* $f = x^6 - 8x^4 - 8x^3 + 8x^2 + 12x - 8$ *and let* $C/\mathbb{Q}$ *be the hyperelliptic curve* $y^2 = f(x)$*. We shall compute the global root number of* $\mathrm{Jac}(C)$*. Note that it has conductor* 13^4 *so* $W(\mathrm{Jac}(C)/\mathbb{Q}) = W(\mathrm{Jac}(C)/\mathbb{Q}_{13})$ *since the root number at the Archimedean place is positive.*

The cluster picture[2] *we associate to* f *at* 13 *is*



where we denote the five roots in the inner cluster $\mathfrak{s}_1$ *by* $\alpha_1, ..., \alpha_4, \beta$ *and the lone root in the outer cluster* $\mathfrak{s}_2$ *by* γ*. Furthermore, the (cyclic) action of inertia on the roots is given by* $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$*.*

	$\mathfrak{s}_1$	$\mathfrak{s}_2$
$d_{\mathfrak{s}}$	$1/4$	0
$\mathfrak{s}^0$	$\{\{\alpha_1\}, \{\alpha_2\}, \{\alpha_3\}, \{\alpha_4\}, \{\beta\}\}$	$\{\mathfrak{s}_1, \{\gamma\}\}$
$I_{\mathfrak{s}}$	I	I
$\mu_{\mathfrak{s}}$	0	0
$\epsilon_{\mathfrak{s}}$	0	$\mathbb{1}$
$\lambda_{\mathfrak{s}}$	$5/8$	0
$\gamma_{\mathfrak{s}}$	*Order* 8 *character* χ	$\mathbb{1}$
$V_{\mathfrak{s}}$	$\chi \oplus \chi^3 \oplus \chi^5 \oplus \chi^7$	0 *representation*

Collating this information, we see that for the abelian variety $\mathrm{Jac}(C)/\mathbb{Q}_{13}$*, we have* $m_8 = 1$ *and* $m_e = m_T = 0$ *otherwise. Therefore*

$$W(\mathrm{Jac}(C)/\mathbb{Q}) = W_{13,8} = \left(\frac{2}{13}\right) = -1,$$

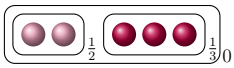
which implies that the Jacobian has odd (and therefore positive) rank, assuming the parity conjecture. It fact, it is known [BSS$^+$*16, Col17, label 28561.a.371293.1] to have analytic rank* 1 *which agrees with our calculation.*

We also give a second example where H^1_t is nonzero to demonstrate the full power of our results.

Example 3.4.6. *Consider the hyperelliptic curve* $C : y^2 = ((x+1)^2 - 11)(x^3 - 11)$

[2]The annotated numbers refer to the depths.

over $\mathbb{Q}_{11}$. The cluster picture this time is



so this curve does not have potentially good reduction since we have a cluster of even cardinality. We have labelled the roots here as

$$\begin{aligned} \alpha_1 &= -1+\sqrt{11},\ \alpha_2 = -1-\sqrt{11}, \\ \beta_1 &= \sqrt[3]{11},\ \beta_2 = \zeta_3\sqrt[3]{11},\ \beta_3 = \zeta_3^2\sqrt[3]{11}, \end{aligned}$$

where we have used the same Greek letter for Galois conjugates. Notice that the Galois conjugates form the subclusters so the stabilisers are the full inertia group.

	$\mathfrak{s}_1$	$\mathfrak{s}_2$	$\mathfrak{s}_3$
$d_{\mathfrak{s}}$	$1/2$	$1/3$	0
$\mathfrak{s}^0$	$\{\{\alpha_1\},\{\alpha_2\}\}$	$\{\{\beta_1\},\{\beta_2\},\{\beta_3\}\}$	$\{\{\beta_1,\beta_2,\beta_3\}\}$
$I_{\mathfrak{s}}$	I	I	I
$\mu_{\mathfrak{s}}$	0	0	0
$\epsilon_{\mathfrak{s}}$	$\mathbb{1}$	0	0
$\lambda_{\mathfrak{s}}$	$1/2$	$1/2$	0
$\gamma_{\mathfrak{s}}$	*Order* 2 *character* η	*Order* 2 *character* η	$\mathbb{1}$

We compute that

$$\begin{aligned} \mathbb{C}[\mathfrak{s}_1^0] &= \mathbb{1}\oplus\eta, \\ \mathbb{C}[\mathfrak{s}_2^0] &= \mathbb{1}\oplus\chi\oplus\chi^2,\ \textit{where}\chi\ \textit{is an order 3 character}, \\ \mathbb{C}[\mathfrak{s}_3^0] &= \mathbb{1}, \end{aligned}$$

and therefore

$$\begin{aligned} V_{\mathfrak{s}_1} &= 0, \\ V_{\mathfrak{s}_2} &= (\chi\otimes\eta)\oplus(\chi\otimes\eta)^{-1}, \\ V_{\mathfrak{s}_3} &= 0. \end{aligned}$$

Hence $H^1_{ab} = (\chi\otimes\eta)\oplus(\chi\otimes\eta)^{-1}$ where $\chi\otimes\eta$ is an order 6 character and we can see from the table above that $H^1_t = \mathbb{1}$.

Since $\chi\otimes\eta$ has order 6, the root number depends on whether -1 is a square in the residue field. In this case, $p = 11$ so the root number for the representation on H^1_{ab} is

-1. *Since H^1_t is trivial, it is unramified so we need to check the Euler factor which tells us that the Weil–Deligne representation is not trivial on Frobenius and therefore root number on this part is* 1.

Combining the two together, we see that $W(\mathrm{Jac}(C)/\mathbb{Q}_{11}) = -1$.

Remark 3.4.7. *In a recent paper of Brumer, Kramer and Sabitova [BKS18], they compute root numbers of a few genus two hyperelliptic curves. Our results combined with the above method of [DDMM] enable us to easily compute all the relevant local root numbers away from* 3. *At* $p = 3$*, their examples have wild inertia but they additionally impose that the curves are potentially totally toric here and hence our results apply directly to their first three examples which have abelian image of inertia. When the image of inertia is non-abelian (it is isomorphic to* S_3*), the machinery of [DDMM] enables us to compute* ρ_T *explicitly and therefore also* $\det \rho_T$. *This is then sufficient to recover the local root number at* 3.

Chapter 4

Twisted root numbers and global applications

4.1 Introduction

We begin this chapter by studying twisted root numbers. Our main result is to prove that for a self-dual Artin twist τ_v, the (local) twisted root number is given by

$$W(A/K, \tau_v) = W(A/K)^{\dim \tau_v}((\det \tau_v)(-1))^{\dim A}(-1)^l,$$

where we explicitly determine l in terms of the invariants we used for $W(A/K)$ in the previous chapter (see Theorem 4.1.1 for the description of l). We are also able to give an analogous formula for the global twisted root number.

This is a refinement of Sabitova's work [Sab07], who only gives a partial description of the twisted root number; our method of proof will use the theory built up in the previous chapter in tandem with her work in order to produce our result. In addition, we use our knowledge of the twisted root number to recover a corresponding summand of the form ρ_e for the original abelian variety.

In §4.4, we give an application of our results by deriving sufficient criteria for abelian varieties with the property that the parity of their rank is invariant under quadratic twist; a table of hyperelliptic curves whose Jacobians have this property is given in Appendix A. Since the rank of an abelian variety $A/\mathcal{K}$ over a quadratic extension $\mathcal{K}(\sqrt{d})/\mathcal{K}$ is the sum of the rank $A/\mathcal{K}$ and the rank of its quadratic twist $A^d/\mathcal{K}$ (cf. Example 2.5.10), this is equivalent globally to saying that $W(A/\mathcal{K}(\sqrt{d})) = 1$. This has an interesting ap-

plication: if $W(A/\mathcal{K}) = -1$, then the rank of $A/\mathcal{K}$ should increase in *every* quadratic extension. In the setting of elliptic curves, Mazur and Rubin conjecture [MR10, Conjecture 1.3] that this root number property is one of only two phenomena[1] that prevent an elliptic curve from having quadratic twists of any given 2-Selmer rank. In particular, this would imply that every elliptic curve over a number field $\mathcal{K}$ has a quadratic twist of rank at most 2; we might expect a similar statement for abelian varieties.

4.1.1 Statement of results

Before we give the results for this chapter, we give a little bit of extra notation, in addition to that from §1.1 and §3.1.1.

Notation.

$\rho_{e,f}$ the direct sum of all faithful irreducible f-dimensional representations of $\mathrm{Gal}(K(\zeta_e, \pi_K^{1/e})/K)$, where $f = [K(\zeta_e) : K]$.

We shall now give the result for the twisted root numbers and a sufficient criterion for the quadratic twist phenomenon. As before, we identify the determinant character $\det \tau_v$ with a character of $K^\times$ under the Artin map.

Theorem 4.1.1 (=Theorem 4.2.10)**.** *Let A/K be an abelian variety over a non-Archimedean local field which has tame reduction and let τ_v be a self-dual Artin representation of $\mathrm{Gal}(\overline{K}/K)$. Then*

$$W(A/K, \tau_v) = W(A/K)^{\dim \tau_v}((\det \tau_v)(-1))^{\dim A}(-1)^{l_1+l_2},$$

where

$$l_1 = \langle \rho_T, \tau_v \rangle + \dim \tau_v \langle \mathbb{1}, \rho_T \rangle,$$

$$l_2 = \sum_{e \in \mathbb{N}} m_e \left(\langle \rho_{e,f}, \tau_v \rangle + \frac{\tilde{\varphi}(e)}{[K(\zeta_e) : K]} (\langle \mathbb{1}, \tau_v \rangle + \langle \eta_v, \tau_v \rangle + \dim \tau_v) \right),$$

with η_v the unramified quadratic character of $K^\times$.

Remark 4.1.2. *For completeness, we give the result for the Archimedean places (see [Sab07, Lemma 2.1]) since we shall use it in the global case. Let $F = \mathbb{R}$ or $\mathbb{C}$ and let τ_v be an Artin representation of $\mathrm{Gal}(\overline{F}/F)$. Then*

$$W(A/F, \tau_v) = (-1)^{(\dim A)(\dim \tau_v)}.$$

[1] The other being the existence of rational 2-torsion points.

We have also collated this into a formula for the global twisted root number.

Theorem 4.1.3 (=Theorem 4.2.11)**.** *Let $\mathcal{K}$ be a global field, $A/\mathcal{K}$ an abelian variety and τ a finite dimensional Artin representation with real character. For each finite place v, write $\rho_{A/\mathcal{K}_v} = \rho_{B_v} \oplus (\rho_{T_v} \otimes \chi_{cyc}^{-1} \otimes \mathrm{sp}(2))$ where ρ_{B_v}, ρ_{T_v} have finite image of inertia. If τ_v is ramified, assume $A/\mathcal{K}_v$ has tame reduction. Then*

$$W(A/\mathcal{K}, \tau) = W(A/\mathcal{K})^{\dim \tau}(\mathrm{sign}(\det \tau))^{\dim A} \cdot T \cdot S,$$

where

$$\begin{aligned}
\mathrm{sign}(\det \tau) &= \prod_{v|\infty,\, v \in M_{\mathcal{K}}} (\det \tau_v)(-1), \\
T &= \prod_{v<\infty, v \in M_{\mathcal{K}}} (-1)^{\langle \rho_{T_v}, \tau_v \rangle + \dim \tau \langle \mathbb{1}, \rho_{T_v} \rangle}, \\
S &= \prod_{v<\infty, v \in M_{\mathcal{K}}} \prod_{e \in \mathbb{N}} \left((-1)^{\langle \rho_{e,f}^v, \tau_v \rangle + \frac{\tilde{\varphi}(e)}{[\mathcal{K}_v(\zeta_e):\mathcal{K}_v]} (\langle \mathbb{1}, \tau_v \rangle + \langle \eta_v, \tau_v \rangle + \dim \tau)} \right)^{m_{e,v}},
\end{aligned}$$

$m_{e,v}$ is the term m_e for ρ_{B_v}, $\rho_{e,f}^v$ is the Artin representation $\rho_{e,f}$ for $\mathrm{Gal}(\overline{\mathcal{K}_v}/\mathcal{K}_v)$ and η_v is the unramified quadratic character of $\mathcal{K}_v^\times$.

As an application of these results, we are also able to provide sufficient criteria for an abelian variety over a global field whose global root number is invariant under quadratic twist. In particular if we can find such an abelian variety with odd rank, then all of its quadratic twists should have infinitely many rational points by the parity conjecture.

Criterion A. Let A/K be an abelian variety over a non-Archimedean local field. Suppose that A/K has tame reduction and that p is odd or ρ_T is zero.

Write

$$\rho_T = \mathbb{1}^{n_1} \oplus \eta^{n_2} \oplus \bigoplus_{j=3}^{m} \chi_j^{n_j} \oplus (\theta \oplus \theta^*),$$

where η, χ_j are all the quadratic characters of K and η is the unique unramified quadratic character. Let $W_g = \prod_{2 \nmid e} W_{q,e}^{m_e} \prod_{e=4 \text{ or } 2||e} W_{q,e/2}^{m_e}$.

Then A/K satisfies Criterion A if any of the following conditions hold:

i. $p = 2$ and $W_g = 1$;

ii. $q \equiv 1 \bmod 4$, $n_3 \equiv \cdots \equiv n_m \bmod 2$ and $W_g = (-1)^{n_2+n_3}$;

iii. $q \equiv 3 \bmod 4$, $n_1 + \cdots + n_m \equiv 0 \bmod 2$ and $W_g = (-1)^{n_2}$.

Theorem 4.1.4 (=Lemma 4.4.4 and Theorem 4.4.5)**.** *Let $A/\mathcal{K}$ be an abelian variety over a global field. Then the global root number of* every *quadratic twist of $A/\mathcal{K}$ is equal if both of the following criteria are satisfied:*

i. $\dim A$ *is even or $\mathcal{K}$ has no real places;*

ii. for every finite place v, $A/\mathcal{K}_v$ satisfies Criterion A.

4.2 The twisted root number

We shall now generalise our results by considering the effect on the root number after twisting ρ_A by an Artin representation τ_v with real character; this implies that the twisted root number will be real.

Firstly, we note that Sabitova [Sab07, Sab13] has previously given formulae for twisted root numbers but these are not currently practical for computational purposes so we shall adapt them using our theory. For completeness, we shall give the relevant propositions we use here.

Proposition 4.2.1. *[Sab07, Proposition 1.5] Let $\mathbb{Z} = \langle \mathrm{Frob} \rangle$, $I = \langle \iota | \iota^e \rangle$, $G = I \rtimes \mathbb{Z}$ where $\mathrm{Frob}\, \iota\, \mathrm{Frob}^{-1} = \iota^q$ with q a unit modulo e. Let f be the least positive integer such that $q^f \equiv 1 \bmod e$. Then every irreducible symplectic representation θ of G which acts faithfully on I, factors through $H = G/\langle \mathrm{Frob}^{2f} \rangle$ and as a representation of H has the form*

$$\theta = \mathrm{Ind}_{I \rtimes \Gamma}^{H} \phi,$$

where $\Gamma \cong C_2$ is the subgroup of $\mathbb{Z}/\langle \mathrm{Frob}^{2f} \rangle$ generated by Frob^f and ϕ is a character of $I \rtimes \Gamma$ such that

i. $\phi(\iota)$ is of order e,

ii. f is even and $q^{f/2} \equiv -1 \bmod e$,

iii. $\phi(\mathrm{Frob}^f) = -1$.

Definition 4.2.2. *Given a representation $\theta = \mathrm{Ind}_{I \rtimes \Gamma}^{H} \phi$ as above, let ν denote the unramified quadratic character of $I \rtimes \Gamma$. We then define*

$$\hat{\theta} = \mathrm{Inf}_{H}^{G} \mathrm{Ind}_{I \rtimes \Gamma}^{H} (\phi \otimes \nu),$$

where Inf_H^G *is the inflation map from* H *to* G*. If* ρ *is an irreducible Weil representation which is not symplectic, we define* $\hat{\rho}$ *to be the zero representation and then extend this definition linearly to all Weil representations.*

The above proposition is already encapsulated in Lemma 3.2.3 and the symplectic representations are precisely those of the form $\theta = \mathrm{Ind}\,\chi \otimes \gamma$ with $\gamma \neq \mathbb{1}$. This allows us to see directly that $\hat{\theta} = \mathrm{Ind}\,\chi$; i.e. the corresponding orthogonal representation. The reason we need to consider this twist is due to the following proposition.

Proposition 4.2.3. *[Sab07, Proof of Proposition 1.9] Let* θ *be a tamely ramified, irreducible, symplectic Weil representation and let* τ_v *be a self-dual Artin representation of* $\mathrm{Gal}(\overline{K}/K)$*. Then*

$$W(\theta \otimes \tau) = ((\det \tau_v)(-1)^{\frac{1}{2}\dim\theta}\chi(u)^{\dim\tau_v}(-1)^{\langle \mathbb{1},\tau_v\rangle+\langle\eta_v,\tau_v\rangle+\langle\hat{\theta},\tau_v\rangle},$$

where η_v *is the unramified quadratic character of* $K^\times$ *and* $\chi(u)$ *is precisely the factor occurring in the Theorem of Fröhlich and Queyrut.*

Remark 4.2.4. *To see directly from the proof that* $\chi(u)$ *is the Fröhlich–Queyrut term, let* $\tau_v = \mathbb{1}$ *and use Lemma 3.2.20.*

Our first step towards a complete formula for the twisted root number is to give an explicit description of $\hat{\theta}$ above. Continuing with our approach of breaking ρ_B into symplectic summands of the form ρ_e, we shall describe the corresponding orthogonal representations attached to each ρ_e. Since Lemma 3.3.1 gives us a direct route to computing the twisted root number for dual pairs, we shall instead concentrate for the moment on the case that each irreducible summand is self-dual of (even) dimension at least 2 (cf. Lemma 3.2.3). This further implies $q \not\equiv 1 \bmod e$ and hence $\zeta_e \notin K$.

Observe that if $\dim\theta = f$ and θ is symplectic, then the orthogonal version $\hat{\theta}$ factors through a Galois extension L/K with $\mathrm{Gal}(L/K) = \langle \iota, \mathrm{Frob} \mid \iota^e, \mathrm{Frob}^f, \mathrm{Frob}\,\iota\,\mathrm{Frob}^{-1} = \iota^q\rangle \cong C_e \rtimes C_f$ with a faithful action. We now explicitly describe L.

Lemma 4.2.5. *Let* $K/\mathbb{Q}_p$ *be a finite extension with residue cardinality* q*. Let* θ *be an irreducible, orthogonal, tamely ramified Weil representation of* $\mathcal{W}(\overline{K}/K)$ *such that* $\dim\theta \geqslant 2$ *and* $\theta(I) = e$*. Then* θ *factors faithfully through* $\mathrm{Gal}(K(\zeta_e, \pi_K^{1/e})/K)$*.*

Proof. Let f be the order of $q \bmod e$. Then by Proposition 4.2.1, every irreducible symplectic representation whose image of inertia has order e factors through $\dfrac{\mathcal{W}(\overline{K}/K)}{\langle \iota^e, \mathrm{Frob}^{2f}\rangle}$, and hence so does θ by Lemma 3.2.29.

Applying Lemma 3.2.3, we find that θ is orthogonal if and only if $\ker\theta = \langle \mathrm{Frob}^f \rangle$ and therefore determines a unique Galois extension of K for which θ can faithfully factor through. A quick check shows that

$$\mathrm{Gal}(K(\zeta_e, \pi_K^{1/e})/K) = \langle \iota, \mathrm{Frob}\,|\iota^e, \mathrm{Frob}^f, \mathrm{Frob}\,\iota\,\mathrm{Frob}^{-1} = \iota^q \rangle \cong C_e \rtimes C_f$$

contains such orthogonal representations and is therefore the desired extension.

□

With our extension L/K determined, we may now describe the $\hat{\theta}$ as Galois representations and not just abstract representations.

Lemma 4.2.6. *Let ρ be a symplectic, tamely ramified Weil representation of the form ρ_e (cf. Definition 3.2.26) for some integer $e > 2$. Assume moreover that every irreducible summand of ρ is symplectic. Then the direct sum of the orthogonal twists, $\hat{\rho}_e$, is isomorphic to the direct sum of all irreducible, faithful, f-dimensional representations of $\mathrm{Gal}(K(\zeta_e, \pi_K^{1/e})/K)$, where $f = [K(\zeta_e) : K]$ is the order of $q \bmod e$.*

Proof. First observe that every irreducible summand θ_j of ρ has dimension f, hence so will $\hat{\theta}_j$ and faithfulness follows from Lemma 3.2.3v. Moreover $\hat{\theta}$ is a one-dimensional twist of θ (cf. Lemma 3.2.29) so is also irreducible. Now observe that distinct summands θ_j of ρ have distinct traces on ι since these are $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugate and sums of primitive e^{th} roots of unity and hence θ_j are also all distinct.

Note that this produces $\tilde{\varphi}(e)/f$ such representations; to finish the proof, we simply need to show that $\mathrm{Gal}(L/K)$ has the same number of representations with these properties, where $L = K(\zeta_e, \pi_K^{1/e})$. Now let θ, θ' be irreducible, faithful representations of $\mathrm{Gal}(L/K)$ and write $\theta = \mathrm{Ind}_{L/L^I}\chi, \theta = \mathrm{Ind}_{L/L^I}\chi'$ as in Lemma 3.2.3 with χ, χ' faithful. Then by the classification of representations of such semidirect products [Ser77, p.62], $\theta \cong \theta'$ if and only if $\chi' = {}^{\mathrm{Frob}^k}\chi$ for some k. Since there are $\tilde{\varphi}(e)$ faithful characters of C_e, the result follows. □

The above lemma prompts us to make the following definition.

Definition 4.2.7. *Let $L = K(\zeta_e, \pi_K^{1/e})$ and $f = f(L/K) = [K(\zeta_e) : K]$. Then $\rho_{e,f}$ is the direct sum of all irreducible, faithful, f-dimensional representations of $\mathrm{Gal}(L/K)$.*

However, since $\hat{\theta}$ only sees irreducible symplectic summands, there is a priori a need to distinguish these not only from the orthogonal ones, but those that are not self-

dual as well. It turns out that such distinctions our unnecessary if we only care about multiplicities $\mathrm{mod}2$, which will be true for twisted root numbers (see Lemma 4.2.9).

Lemma 4.2.8. *Let $\rho = \bigoplus_j \rho_{e_j}$ be tamely ramified, symplectic Weil representation where ρ_{e_j} are of the form ρ_e. Then for all self-dual Artin representations τ_v of $\mathrm{Gal}(\overline{K}/K)$:*

$$\langle \hat{\rho}, \tau_v \rangle \equiv \sum_j \langle \rho_{e_j,f_j}, \tau_v \rangle \bmod 2,$$

where f_j is the order of $q \bmod e_j$.

Proof. First note that if every irreducible summand of ρ is symplectic, then we have equality by Lemma 4.2.6. All irreducible summands θ of ρ which are not symplectic give no contribution to $\hat{\rho}$, so we must show that they always occur with even multiplicity in τ. Observe first that if θ does not have finite image, then θ is trivially not a subrepresentation of τ and we may restrict ourselves to θ of Galois type which are not symplectic.

By Lemma 3.2.30, $\theta \oplus \theta^*$ is a subrepresentation of ρ and hence $\bigoplus_j \rho_{e_j,f_j} = \hat{\rho} \oplus \theta_1 \oplus \theta_1^*$, where each irreducible summand of θ_1 is orthogonal or not self-dual. We claim that for any self-dual Artin representation τ_v, we have $\langle \theta_1, \tau_v \rangle = \langle \theta_1^*, \tau_v \rangle$. This is trivial for the irreducible self-dual summands; the other case follows since τ is self-dual. Hence

$$\begin{aligned}
\sum_j \langle \rho_{e_j,f_j}, \tau_v \rangle &= \langle \bigoplus_j \rho_{e_j,f_j}, \tau_v \rangle, \\
&= \langle \hat{\rho} \oplus \theta_1 \oplus \theta_1^*, \tau_v \rangle, \\
&= \langle \hat{\rho}, \tau_v \rangle + 2\langle \theta_1, \tau_v \rangle, \\
&\equiv \langle \hat{\rho}, \tau_v \rangle \bmod 2.
\end{aligned}$$

□

With the $\hat{\rho}$ described, we can now focus on the twisted root numbers themselves.

Lemma 4.2.9. *Let ρ be a tamely ramified Weil representation and let ρ_T, τ_v be self-dual Artin representations. Then:*

i. $W(\rho_T \otimes \tau_v \otimes \mathrm{sp}(2)) = W(\rho_T \otimes \mathrm{sp}(2))^{\dim \tau_v}((\det \tau_v)(-1))^{\dim \rho_T}(-1)^{\langle \rho_T, \tau_v \rangle + \dim \tau_v \langle \mathbb{1}, \rho_T \rangle}$;

ii. $W((\rho \oplus \rho^*) \otimes \tau_v) = W(\rho \oplus \rho^*)^{\dim \tau_v}((\det \tau_v)(-1))^{\dim \rho}$;

iii. If ρ is irreducible and symplectic, then

$$W(\rho \otimes \tau_v) = W(\rho)^{\dim \tau_v}((\det \tau_v)(-1))^{\frac{1}{2}\dim \rho}(-1)^{\dim \tau_v + \langle \mathbb{1}, \tau_v\rangle + \langle \eta_v, \tau_v\rangle + \langle \hat{\rho}, \tau_v\rangle},$$

where η_v is the quadratic unramified character of $K^\times$.

Proof. (i): Observe that $\rho_T \otimes \tau$ is self-dual and hence has real character so we may apply Lemma 3.3.1. Hence

$$\begin{aligned} W(\rho_T \otimes \tau_v \otimes \mathrm{sp}(2)) &= (-1)^{\langle \mathbb{1}, \rho_T \otimes \tau_v\rangle}((\det \rho_T \otimes \tau_v)(-1)), \\ &= (-1)^{\langle \rho_T, \tau_v\rangle}((\det \rho_T)(-1))^{\dim \tau_v}((\det \tau_v)(-1))^{\dim \rho_T}, \\ &= W(\rho_T \otimes \mathrm{sp}(2))^{\dim \tau_v}((\det \tau_v)(-1))^{\dim \rho_T}(-1)^{\langle \rho_T, \tau_v\rangle + \dim \tau_v \langle \mathbb{1}, \rho_T\rangle}, \end{aligned}$$

where on the second line we note that $\langle \mathbb{1}, \sigma_1 \otimes \sigma_2\rangle = \langle \sigma_1, \sigma_2\rangle$ for all Artin representations σ_1, σ_2 with real character.

(ii): As τ_v is self-dual, $(\rho \oplus \rho^*) \otimes \tau_v \cong (\rho \otimes \tau_v) \oplus (\rho \otimes \tau_v)^*$. We may therefore apply Corollary 2.2.6 to obtain:

$$\begin{aligned} W((\rho \oplus \rho^*) \otimes \tau_v) &= \det(\rho \otimes \tau_v)(-1), \\ &= ((\det \rho)^{\dim \tau_v}(-1))((\det \tau_v)^{\dim \rho}(-1)), \\ &= W(\rho \oplus \rho^*)^{\dim \tau_v}((\det \tau_v)(-1))^{\dim \rho}. \end{aligned}$$

(iii): By Proposition 4.2.3, $W(\rho \otimes \tau) = ((\det \tau)(-1)^{\frac{1}{2}\dim \rho}\chi(u)^{\dim \tau}(-1)^{\langle \mathbb{1}, \tau_v\rangle + \langle \eta_v, \tau_v\rangle + \langle \hat{\rho}, \tau_v\rangle}$. Making the substitution $W(\rho) = -\chi(u)$ (cf. Lemma 3.2.20) yields the result. □

Theorem 4.2.10. *Let A/K be an abelian variety over a non-Archimedean local field which has tame reduction and let τ_v be a self-dual Artin representation of $\mathrm{Gal}(\overline{K}/K)$. Write $\rho_A = \rho_B \oplus (\rho_T \otimes \chi_{cyc}^{-1} \otimes \mathrm{sp}(2))$ as in Fact 2.3.2. Moreover, write $\rho_B \otimes \chi_{cyc}^{1/2} = \bigoplus_j \rho_{e_j}$ as a decomposition of summands of the form ρ_e (cf. Definition 3.2.26) and let $m_e = |\{j : e_j = e\}|$ count the multiplicity of such summands.*

Then

$$W(A/K, \tau_v) = W(A/K)^{\dim \tau_v}((\det \tau_v)(-1))^{\dim A}(-1)^{l_1 + l_2},$$

where

$$l_1 = \langle \rho_T, \tau_v\rangle + \dim \tau_v \langle \mathbb{1}, \rho_T\rangle,$$

$$l_2 = \sum_{e \in \mathbb{N}} m_e \left(\langle \rho_{e,f}, \tau_v\rangle + \frac{\tilde{\varphi}(e)}{[K(\zeta_e) : K]}(\langle \mathbb{1}, \tau_v\rangle + \langle \eta, \tau_v\rangle + \dim \tau_v) \right),$$

with η_v the unramified quadratic character of $K^\times$ and for a fixed $e \in \mathbb{N}$, $f = [K(\zeta_e) : K]$ is the order of $q \bmod e$.

Proof. First note that $W(\rho_A \otimes \tau_v) = W(\rho_B \otimes \chi_{cyc}^{1/2} \otimes \tau_v) W(\rho_T \otimes \tau_v \otimes \mathrm{sp}(2))$ by Corollary 2.2.6 and that $W(\rho_T \otimes \tau_v \otimes \mathrm{sp}(2))$ is completely described by Lemma 4.2.9 and recovers the term l_1.

We now study $\rho_B \otimes \chi_{cyc}^{1/2} = \bigoplus_j \rho_{e_j}$. Observe that for any irreducible summand ρ which is not symplectic, $\rho \oplus \rho^*$ is a subrepresentation and by Lemma 4.2.9

$$W((\rho \oplus \rho^*) \otimes \tau_v) = W(\rho \oplus \rho^*)^{\dim \tau_v} ((\det \tau_v)(-1))^{\dim \rho} (-1)^{2 \dim \tau_v + 2\langle \mathbb{1}, \tau_v \rangle + 2\langle \eta_v, \tau_v \rangle + 2\langle \hat{\rho}, \tau_v \rangle},$$

since $\hat{\rho} = \hat{\rho^*}$ is the zero representation.

Since $\dfrac{W((\rho \oplus \rho^*) \otimes \tau_v)}{W(\rho \oplus \rho^*)^{\dim \tau_v}}$ only depends on $\dim \rho$ (and not whether ρ is orthogonal, symplectic or not self-dual) and the non-symplectic summands always arise in this way, we obtain

$$\frac{W(\rho_B \otimes \chi_{cyc}^{1/2} \otimes \tau_v)}{W(\rho_B \otimes \chi_{cyc}^{1/2})^{\dim \tau_v}} = ((\det \tau_v)(-1))^{\frac{1}{2} \dim \rho_B} (-1)^{m \dim \tau_v + m\langle \mathbb{1}, \tau_v \rangle + m\langle \eta_v, \tau_v \rangle + \langle \bigoplus_j \hat{\rho}_{e_j}, \tau_v \rangle},$$

where m is the number of irreducible summands of $\rho_B \otimes \chi_{cyc}^{1/2}$.

For a fixed subrepresentation ρ_e, observe that each irreducible summand has dimension $f = [K(\zeta_e) : K]$ (the order of $q \bmod e$) and hence ρ_e has $\frac{\tilde{\varphi}(e)}{[K(\zeta_e):K]}$ summands. Moreover, there are m_e such representations of the form ρ_e so we get

$$\frac{W(\rho_B \otimes \chi_{cyc}^{1/2} \otimes \tau_v)}{W(\rho_B \otimes \chi_{cyc}^{1/2})^{\dim \tau_v}} = ((\det \tau_v)(-1))^{\frac{1}{2} \dim \rho_B} (-1)^l,$$

where $l = \langle \bigoplus_j \hat{\rho}_{e_j}, \tau_v \rangle + \sum_{e \in \mathbb{N}} m_e \left(\dfrac{\tilde{\varphi}(e)}{[K(\zeta_e) : K]} (\langle \mathbb{1}, \tau_v \rangle + \langle \eta, \tau_v \rangle + \dim \tau_v) \right)$. Furthermore, $(-1)^{\langle \bigoplus_j \hat{\rho}_{e_j}, \tau_v \rangle} = (-1)^{\sum_j \langle \rho_{e_j, f_j}, \tau_v \rangle}$ by Lemma 4.2.8 hence $l = l_2$.

Collating the above computations, we have

$$\begin{aligned} \frac{W(\rho_A \otimes \tau_v)}{W(\rho_B \otimes \chi_{cyc}^{1/2})^{\dim \tau_v} W(\rho_T \otimes \mathrm{sp}(2))^{\dim \tau_v}} &= ((\det \tau_v)(-1))^{\frac{1}{2} \dim \rho_B + \dim \rho_T} (-1)^{l_1 + l_2}, \\ &= ((\det \tau_v)(-1))^{\dim A} (-1)^{l_1 + l_2}, \end{aligned}$$

where we have used that $\frac{1}{2} \dim \rho_B + \dim \rho_T = \frac{1}{2} \dim \rho_A = \dim A$. Lastly, the additivity

property of root numbers together with Corollary 2.2.6 shows that

$$W(\rho_B \otimes \chi_{cyc}^{1/2}) W(\rho_T \otimes \mathrm{sp}(2)) = W(\rho_A)$$

and completes the proof. □

4.2.1 The global case

We now wish to look at the contribution of a global twist τ, using our relation in Theorem 4.2.10. To consider the global contribution, we should also take into account the infinite places (cf. Remark 4.1.2). Observe that for each finite place, we obtained a factor of $((\det \tau_v)(-1))^{\dim A}$. Viewing $\det \tau$ as an adelic character which is trivial on $\mathbb{Q}^\times$ instead, we see that

$$\mathrm{sign}(\det \tau) := \prod_{v|\infty,\, v \in M_{\mathcal{K}}} (\det \tau_v)(-1) = \prod_{v<\infty,\, v \in M_{\mathcal{K}}} (\det \tau_v)(-1).$$

Recall that we define

$$W(A/\mathcal{K}, \tau) := \prod_{v \in M_{\mathcal{K}}} W(A/\mathcal{K}_v, \tau_v),$$

where $M_{\mathcal{K}}$ is the set of all places of $\mathcal{K}$.

Theorem 4.2.11. *Let $\mathcal{K}$ be a global field, $A/\mathcal{K}$ an abelian variety and τ a finite dimensional Artin representation with real character. For each finite place v, write $\rho_{A/\mathcal{K}_v} = \rho_{B_v} \oplus (\rho_{T_v} \otimes \chi_{cyc}^{-1} \otimes \mathrm{sp}(2))$ where ρ_{B_v}, ρ_{T_v} have finite image of inertia. If τ_v is ramified, assume $A/\mathcal{K}_v$ has tame reduction. Then*

$$W(A/\mathcal{K}, \tau) = W(A/\mathcal{K})^{\dim \tau} (\mathrm{sign}(\det \tau))^{\dim A} \cdot T \cdot S,$$

where

$$\begin{aligned}
\mathrm{sign}(\det \tau) &= \prod_{v|\infty,\, v \in M_{\mathcal{K}}} (\det \tau_v)(-1), \\
T &= \prod_{v<\infty, v \in M_{\mathcal{K}}} (-1)^{\langle \rho_{T_v}, \tau_v \rangle + \dim \tau \langle \mathbb{1}, \rho_{T_v} \rangle}, \\
S &= \prod_{v<\infty, v \in M_{\mathcal{K}}} \prod_{e \in \mathbb{N}} \left((-1)^{\langle \rho_{e,f}^v, \tau_v \rangle + \frac{\tilde{\varphi}(e)}{[\mathcal{K}_v(\zeta_e) : \mathcal{K}_v]} (\langle \mathbb{1}, \tau_v \rangle + \langle \eta_v, \tau_v \rangle + \dim \tau)} \right)^{m_{e,v}},
\end{aligned}$$

$m_{e,v}$ is the multiplicity of representations ρ_e which are subrepresentations of ρ_{B_v} (as defined previously in Definition 3.2.26), $\rho_{e,f}^v$ is the Artin representation $\rho_{e,f}$ for $\mathrm{Gal}(\overline{\mathcal{K}_v}/\mathcal{K}_v)$ (Definition 4.2.7) and η_v is the unramified quadratic character of $\mathcal{K}_v^\times$.

Proof. This is a straightforward consequence of Theorem 4.2.10. □

Remark 4.2.12. *Note that in the dual case, both $\tilde{\varphi}(e)/[\mathcal{K}_v(\zeta_e) : \mathcal{K}_v]$ and $\langle \rho_{e,f}, \tau_v \rangle$ are even so S has no contribution from such summands (cf. Lemma 3.2.3iv).*

Corollary 4.2.13. *[Sab13, Proposition 1] Let $\mathcal{K}$ be a global field, $A/\mathcal{K}$ an abelian variety and τ a self-dual Artin representation of $\mathrm{Gal}(\overline{\mathcal{K}}/\mathcal{K})$. Assume the conductor $\mathfrak{N}$ of $A/\mathcal{K}$ is coprime to the conductor of τ. Then*

$$W(A/\mathcal{K}, \tau) = W(A/\mathcal{K})^{\dim \tau}((\det \tau)(\mathfrak{N}))(\mathrm{sign}(\det \tau))^{\dim A}.$$

4.3 Recovering ρ_A

Before considering the twisted root number globally, we shall use the theory we've developed so far to reconstruct certain summands of ρ_A.

Proposition 4.3.1. *Let A/K be an abelian variety and suppose that ρ_A is tamely ramified. Write $\rho_A = \rho_B \oplus (\rho_T \otimes \chi_{cyc}^{-1} \otimes \mathrm{sp}(2))$ as in Fact 2.3.2 assume the eigenvalues (or their orders) including multiplicity of $\rho_B(\iota), \rho_B(\iota)$ are known. Then $\rho_A(I)$ is completely determined.*

Proof. This is trivial from the fact that $\rho_A(I)$ is necessarily abelian. □

We briefly mention that we can reconstruct a symplectic representation of the form ρ_e from our $\rho_{e,f}$ in the self-dual case and relate this to a subrepresentation of $\rho_B \otimes \chi_{cyc}^{-1}$.

Proposition 4.3.2. *Let $e \in \mathbb{N}$ be such that $p \nmid e$ and the order f of $q \bmod e$ is such that $f \geqslant 2$ is even and $q^{f/2} \equiv -1 \bmod e$. Let ν be an unramified character of order $2f$. Then $\rho_{e,f} \otimes \nu$ is a symplectic Weil representation ρ of the form ρ_e such that every irreducible summand is also symplectic.*

Moreover, if B/K is an abelian variety with tame, potentially good reduction such that $\rho_B(\iota)$ has an eigenvalue e, then $\rho_B \otimes \chi_{cyc}^{1/2}$ has a subrepresentation of the form ρ_e built from the irreducible summands of ρ and $\rho_{e,f}$. In particular, if every summand of the subrepresentation of the form ρ_e is symplectic, then it is isomorphic to ρ.

Proof. Recall that by construction, every irreducible summand of $\rho_{e,f}$ is orthogonal and hence every summand of $\rho_{e,f} \otimes \nu$ is symplectic by Lemma 3.2.29. Since the conditions on e force irreducible summands to be self-dual and there are exactly two choices (a symplectic or orthogonal choice), the rest of the proposition follows. □

4.4 All quadratic twists with equal parity

There are three different notions of parity for an abelian variety: analytic parity via the root number; parity of the rank of the Mordell–Weil group; and parity of the p^∞-Selmer group for a given prime p (referred to as p-parity). These are equivalent subject to the conjectures of Shafarevich-Tate and Birch–Swinnerton-Dyer. The equivalence of analytic parity and p-parity has been proven for elliptic curves over $\mathbb{Q}$ [DD10, Theorem 1.4]; Morgan has also shown equivalence to 2-parity for Jacobians of hyperelliptic curves over particular quadratic extensions [Mor15, Theorem 1.1].

Example 4.4.1. *[MR10, Example 9.2] Let $E/\mathcal{K}$ be an elliptic curve over a number field with complex multiplication defined over $\mathcal{K}$. Then the global root number of any quadratic twist $W(E'/\mathcal{K})$ is equal to $W(E/\mathcal{K})$; the same statement for 2-parity and parity of the ranks of $E'(\mathcal{K})$ is true.*

Mazur and Rubin have previously determined necessary conditions for an elliptic curve whose quadratic twists all have equal 2-Selmer parity: $\mathcal{K}$ must be totally imaginary and $E/\mathcal{K}$ has good or additive reduction everywhere [MR10, Theorem 9.5]. On the other hand, the Dokchitsers have shown that this 2-parity phenomenon holds for elliptic curves if and only if the equivalent root number statement does [DD11, Corollary 1.6]. They have further derived necessary and sufficient conditions in this case [DD09a, Theorem 1]. We now extend their result to abelian varieties, continuing in the terminology of [DD09a].

Definition 4.4.2. *Let $A/\mathcal{K}$ be an abelian variety over a local or global field. Then we call $A/\mathcal{K}$* lawful *if $W(A/\mathcal{F}) = 1$ for every quadratic extension $\mathcal{F}/\mathcal{K}$. We say a curve is lawful if its Jacobian is.*

Lemma 4.4.3. *Let $A/\mathcal{K}$ be an abelian variety over a global field. Then $A/\mathcal{K}$ is lawful if and only if $W(A/\mathcal{K}) = W(A^\chi/\mathcal{K})$ for every quadratic character χ, where A^χ denotes the quadratic twist of $A/\mathcal{K}$ by χ.*

Proof. Fix a quadratic character χ and let $\mathcal{F}$ be the quadratic extension of $\mathcal{K}$ through

which χ factors. Then on the level of the corresponding ℓ-adic representations, we have $\rho_{A/\mathcal{F}} = \mathrm{Res}_{\mathcal{F}/\mathcal{K}}\, \rho_{A/\mathcal{K}}$ and $\mathrm{Ind}_{\mathcal{F}/\mathcal{K}}\, \rho_{A/\mathcal{F}} = \rho_{A/\mathcal{K}} \oplus \rho_{A^\chi/\mathcal{K}}$. By the inductivity property (Theorem 2.2.1ii), we have

$$\frac{W(\rho_{A/\mathcal{F}})}{W(\mathbb{1}_{\mathcal{F}})^{2\dim A}} = \frac{W(\rho_{A/\mathcal{K}})W(\rho_{A^\chi/\mathcal{K}})}{W(\mathbb{1}_{\mathcal{K}})^{2\dim A}W(\chi)^{2\dim A}},$$

where $\mathbb{1}_{\mathcal{K}}, \mathbb{1}_{\mathcal{F}}$ denote the trivial characters of $\mathcal{F}, \mathcal{K}$ respectively.

Now $W(\mathbb{1}_{\mathcal{K}}) = W(\mathbb{1}_{\mathcal{F}}) = 1$ and since χ is quadratic we have $W(\chi)^{2\dim A} = W(\chi \oplus \chi^*)^{\dim A} = (\chi(-1))^{\dim A}$ and hence

$$W(A/\mathcal{F}) = W(A/\mathcal{K})W(A^\chi/\mathcal{K})(\chi(-1))^{\dim A}.$$

Since $\mathcal{K}$ is a global field, $\chi(-1) = 1$ and the result follows. □

Observe that $A/\mathcal{K}$ is lawful if and only if $A/\mathcal{K}_v$ is lawful for all places v of $\mathcal{K}$.[2] Lawful abelian varieties $A/\mathcal{K}$ come in two flavours depending on $W(A/\mathcal{K})$: *lawful evil* if $W(A/\mathcal{K}) = -1$ and *lawful good* if $W(A/\mathcal{K}) = 1$. Note that the lawful evil case implies that the Mordell–Weil rank should increase in *every* quadratic extension. We list some examples of lawful genus two hyperelliptic curves in Appendix A.

Lemma 4.4.4. *Let $\mathcal{K}$ be a number field and $A/\mathcal{K}$ be lawful. Then either $\dim A$ is even or $\mathcal{K}$ has no real places.*

Proof. Suppose not and let v be a real place, so that $A/\mathcal{K}_v$ is also lawful and let $\mathcal{F}_v \cong \mathbb{C}$ be the unique quadratic extension of $\mathcal{K}_v$. However $W(A/\mathcal{F}_v) = (-1)^{\dim A} = -1$ which contradicts $A/\mathcal{K}$ being lawful. □

Theorem 4.4.5. *Let A/K be an abelian variety over a non-Archimedean local field. Write $\rho_{A/K} = \rho_{B/K} \oplus (\rho_{T,K} \otimes \chi_{cyc}^{-1} \otimes \mathrm{sp}(2))$. Assume that $\rho_{B/K}$ is tamely ramified and $\rho_{T,K}$ is abelian. If A/K doesn't have potentially good reduction, then further assume that the cardinality q of the residue field of K is odd*[3].

[2] If $A/\mathcal{K}_v$ is not lawful for some v, then by imposing only finitely many local conditions we can find a quadratic extension of $\mathcal{K}$ with negative root number.

[3] This is to omit the case where $p = 2$ and $\rho_{T,K}$ is ramified; in this case we would have to further determine which ramified quadratic characters were subrepresentations since they do not all act non-trivially on -1.

Write

$$\begin{aligned}\rho_{B/K} \otimes \chi_{cyc}^{-1/2} &= \bigoplus_{e\in\mathbb{N}} \rho_e^{m_e},\\ \rho_{T,K} &= \mathbb{1}^{n_1} \oplus \eta^{n_2} \oplus \bigoplus_{j=3}^{m} \chi_j^{n_j} \oplus (\theta \oplus \theta^*),\end{aligned}$$

where η, χ_j are all the quadratic characters and η is the unique unramified quadratic character.

Let $W_g = \prod_{2\nmid e} W_{q,e}^{m_e} \prod_{e=4 \text{ or } 2\|e} W_{q,e/2}^{m_e}$.

(i) If $p = 2$, then A/K is lawful if and only if $W_g = 1$.

(ii) If $q \equiv 1 \bmod 4$, then A/K is lawful if and only if $n_1 \equiv n_2 \bmod 2$, $n_3 \equiv \cdots \equiv n_m \bmod 2$ and $W_g = (-1)^{n_2+n_3}$.

(iii) If $q \equiv 3 \bmod 4$, then A/K is lawful if and only if $n_1 + \cdots + n_m \equiv 0 \bmod 2$ and $W_g = (-1)^{n_2}$.

Proof. Let F/K be a quadratic extension and consider first $\rho_{B/K}$. If F/K is unramified, then $W(\rho_{B/F}) = 1$. Otherwise F/K is ramified, so write $\rho_{B/K} \otimes \chi_{cyc}^{-1/2} = \bigoplus \rho_e^{m_e}$. Recall that e is the order of the ramified character and therefore the ramification degree of the Galois extension that $\rho_{e,f}$ factors through. If $2 \nmid e$, then the order and extension are unchanged so this summand still appears in $\rho_{B/K} \otimes \chi_{cyc}^{-1/2}$.

Otherwise, $2|e$ so the order of the character required over F is now $e/2$; hence we replace the summand by $\tilde{\varphi}(e)/\tilde{\varphi}(e/2)$ summands of the form $\rho_{e/2}$. Furthermore, if $4|e$ with $e > 4$, then $\tilde{\varphi}(e) = 2\tilde{\varphi}(e/2)$ so these two summands cancel and therefore $W(\rho_{B/F}) = W_g$.

We now focus on $W(\rho_{T,F} \otimes \chi_{cyc}^{-1} \otimes \mathrm{sp}(2))$. Recall that the root number here only depends on the trivial and quadratic characters, so the term $\theta \oplus \theta^*$ does not affect our calculation.

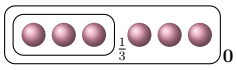
If F/K is unramified, then $W(\rho_{T,F} \otimes \mathrm{sp}(2)) = (-1)^{n_1+n_2} \left(\dfrac{-1}{q}\right)^a$, where $a = n_3 + \cdots + n_m$. On the other hand, each possible quadratic ramified extension corresponds to one of the characters χ_j, so we get a relation for each one:

$$W(\rho_{T,F} \otimes \mathrm{sp}(2)) = (-1)^{n_1+n_j} \left(\frac{-1}{q}\right)^{(a-n_j)}.$$

Collating this information yields the given congruences, taking into account the unramified case as well. □

Example 4.4.6. *Consider the hyperelliptic curve*[4] $C/\mathbb{Q} : y^2 = x^6 - 10x^4 + 2x^3 + 21x^2 - 18x + 5$ *whose Jacobian has conductor* 103^2*. We shall show that its Jacobian is lawful.*

Note that by Lemma 4.4.4 we only need to check the finite places and moreover if $\mathrm{Jac}(C)/\mathbb{Q}_p$ *has good reduction at some prime* $p < \infty$*, then it will have good reduction over any finite extension* $F/\mathbb{Q}_p$ *and therefore* $W(\mathrm{Jac}(C)/F) = 1$*. Therefore the only prime where we have to check the conditions of Theorem 4.4.5 is* 103*. The cluster picture of* $C/\mathbb{Q}_{103}$ *is*



from which we find that it has potentially good reduction (so $n_j = 0$ *for all* j*) and hence* $\mathrm{Jac}(C)/\mathbb{Q}_{103}$ *is lawful if and only if* $W_g = 1$*. Moreover, we compute that* $m_1 = m_6 = 1$ *and* $m_e = 0$ *otherwise and find that*

$$W_g = W_{103,6/2} = \left(\frac{103}{3}\right) = 1.$$

Hence $\mathrm{Jac}(C)/\mathbb{Q}_{103}$ *(and therefore also* $\mathrm{Jac}(C)/\mathbb{Q}$*) is lawful; we moreover check that* $W(\mathrm{Jac}(C)/\mathbb{Q}) = W(\mathrm{Jac}(C)/\mathbb{Q}_{103}) = -1$ *and therefore it is lawful evil.*

Remark 4.4.7. *Note that Lemma 4.4.4 prevents any lawful elliptic curves over* $\mathbb{Q}$*. Consider instead the Weil restriction to* $\mathbb{Q}$ *of a lawful elliptic curve* E/K*, where* K *is a (necessarily imaginary) quadratic number field: this is a two-dimensional abelian variety* $A/\mathbb{Q}$*. Furthermore,* $A/\mathbb{Q}$ *is lawful since* $\rho_A = \mathrm{Ind}_{K/\mathbb{Q}}\,\rho_E$ *[Mil72, p.178(a)] and global root numbers are invariant under induction.*

Now $A/\mathbb{Q}$ *is* $\overline{\mathbb{Q}}$*-isogenous to a product of elliptic curves and therefore cannot be simple. Our example above can however be shown to be simple (by applying Stoll's criterion [Sto95, p.1343-1344] at* $p = 3$*) and is therefore a genuinely new example which is not just the Weil restriction of a lawful elliptic curve.*

[4]The minimal equation for this curve is actually $y^2 + (x^3 + x + 1)y = -3x^4 + 5x^2 - 5x + 1$ but the cluster machinery we use to obtain the root number requires the curve to be in the form $y^2 = f(x)$. Its LMFDB label [Col17] is 10609.b.10609.1.

Chapter 5

Compatibility of the Birch–Swinnerton-Dyer conjecture and Schur indices

5.1 Introduction

There is a standard "minimalist conjecture" that generically the L-function of an elliptic curve vanishes to order 0 or 1 at $s=1$, depending on the sign in the functional equation. As we will illustrate, this has to be used with some caution: even when the associated Galois representation is irreducible, certain L-functions cannot vanish to order 1 at $s=1$ — the order of their zero should be a multiple of a (possibly large) integer n. We do this by considering twisted L-functions and choosing our Artin twist carefully.

Similarly to Chapter 4, we study the twisted L-functions by virtue of the Birch–Swinnerton-Dyer conjecture for Artin twists (Conjecture 2.5.11). However, we do this in a more general setting when our twist is not self-dual and therefore the twisted parity conjecture (Conjecture 2.5.12) is unavailable to us. We find that such phenomenon should arise in a more general setting and investigate its consequences.

If $A/\mathcal{K}$ is an abelian variety, then recall that for a Galois extension $\mathcal{F}/\mathcal{K}$, we may form the complex Galois representation $A(\mathcal{F})_{\mathbb{C}}$. Note that this is actually the extension of a scalars of a rational representation since $A(\mathcal{F})$ is originally a $\mathbb{Z}$-module. We exploit this rationality property by noting that not every representation can be defined over $\mathbb{Q}$ or even its character field. Indeed, the faithful, absolutely irreducible representation τ of the quaternion group Q_8 has rational trace but cannot be realised using rational

matrices; in fact, every rational representation necessarily contains an even number of copies of τ. This can then be translated to an analytic statement: the order of vanishing of $L(A/\mathcal{K}, \tau, s)$ is always even. In this particular case, one could analyse this statement using the twisted root number $W(A/\mathcal{K}, \tau)$ (as we did in Chapter 4) since τ is self-dual. We no longer restrict ourselves to self-dual representations to study this phenomenon and therefore give statements directly concerning the twisted L-function, rather than the twisted root number.

5.2 Making the analytic rank divisible by p

Notation. Throughout this chapter, p and q will be distinct odd primes (unlike the previous two chapters).

Theorem 5.2.1. *Let $E/\mathbb{Q}$ be an elliptic curve. Let τ be an irreducible faithful Artin representation of a Galois extension $\mathcal{F}/\mathbb{Q}$ with $\mathrm{Gal}(\mathcal{F}/\mathbb{Q}) \cong C_q \rtimes C_{p^n}$ non-abelian and with $p^n \nmid q-1$.*
(i) If the Birch–Swinnerton-Dyer conjecture for Artin twists (Conjecture 2.5.11) holds, then

$$\mathrm{ord}_{s=1} L(E/\mathbb{Q}, \tau, s) \equiv 0 \mod p.$$

(ii) If the ℓ-primary part of the Tate–Shafarevich group $Ш(E/\mathcal{F})[\ell^\infty]$ is finite, then

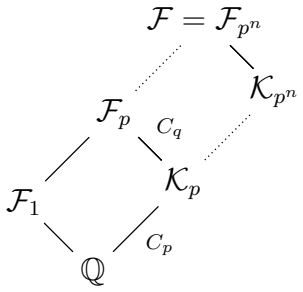
$$\langle X_\ell(E/\mathcal{F}), \tau \rangle \equiv 0 \mod p,$$

where ℓ is any prime and $X_\ell(E/\mathcal{F})$ is the Pontryagin dual of the ℓ^∞-Selmer group of $E/\mathcal{F}$ tensored with $\mathbb{Q}_\ell$, viewed as a representation of $\mathrm{Gal}(\mathcal{F}/\mathbb{Q})$.

This result follows from Theorem 5.3.5 and Theorem 5.4.2(iii). The main question we would like to raise, of course, is whether this behaviour of L-functions or Selmer groups can be explained without appealing to the conjectures.

It is reasonably straightforward to construct such Galois extensions $\mathcal{F}/\mathbb{Q}$.

Consider for simplicity the case when C_{p^n} acts on C_q through C_p. Such fields $\mathcal{F} = \mathcal{F}_{p^n}$ are constructed as the compositum of a C_{p^n}-extension $\mathcal{K}_{p^n}/\mathbb{Q}$ and an extension $\mathcal{F}_p/\mathbb{Q}$ with Galois group $C_q \rtimes C_p$ that shares a common degree p subfield $\mathcal{K}_p$ with $\mathcal{K}_{p^n}$. The irreducible faithful Artin representations of $\mathrm{Gal}(\mathcal{F}/\mathbb{Q})$ are all of the form $\tau \otimes \chi$, for any irreducible p-dimensional representation of $\mathrm{Gal}(\mathcal{F}_p/\mathbb{Q})$ and any 1-dimensional representation χ of $\mathrm{Gal}(\mathcal{K}_{p^n}/\mathbb{Q})$ of order p^n (see Proposition 5.4.1).



For example, $\mathcal{K}_{p^n}$ could be the n^{th} layer of the p-cyclotomic tower of $\mathbb{Q}$, that is the unique degree p^n subfield of $\mathbb{Q}(\zeta_{p^{n+1}})$. This gives the following:

Corollary 5.2.2. *Suppose that $\mathcal{F}_p/\mathbb{Q}$ is Galois with $\mathrm{Gal}(\mathcal{F}_p/\mathbb{Q}) \cong C_q \rtimes C_p$ non-abelian, and that its degree p subfield $\mathcal{K}_p$ is the first layer of the p-cyclotomic extension of $\mathbb{Q}$. Let $E/\mathbb{Q}$ be an elliptic curve and τ an irreducible faithful representation of $\mathrm{Gal}(\mathcal{F}_p/\mathbb{Q})$. If Conjecture 2.5.11 holds, then for all finite order characters χ that factor through the p-cyclotomic extension with $\chi^{q-1} \neq \mathbb{1}$,*

$$\mathrm{ord}_{s=1}\, L(E/\mathbb{Q}, \tau \otimes \chi, s) \equiv 0 \mod p.$$

If τ is a representation of $\mathrm{Gal}(\mathcal{F}/\mathbb{Q})$ such that $\tau = \mathrm{Ind}_{\mathcal{K}/\mathbb{Q}}\, \psi$ for some subfield $\mathcal{K} \subset \mathcal{F}$, then we have an equality of L-functions $L(E/\mathbb{Q}, \tau, s) = L(E/\mathcal{K}, \psi, s)$ for any elliptic curve $E/\mathbb{Q}$. In our setup, all irreducible faithful representations τ are induced from characters. More concretely, if $\mathrm{Gal}(\mathcal{F}_{p^n}/\mathbb{Q}) \cong C_q \rtimes C_{p^n}$ is non-abelian, such that C_{p^n} acts on C_q through C_p, then $\tau = \mathrm{Ind}_{\mathcal{K}_p/\mathbb{Q}}\, \psi$ where $\mathcal{K}_p$ is the degree p subfield of $\mathcal{F}_{p^n}$ and ψ is a primitive character of order qp^{n-1}. In particular, we get the following consequence for L-functions of certain modular forms.

Corollary 5.2.3. *Suppose that $\mathcal{F}_p/\mathbb{Q}$ is Galois with $\mathrm{Gal}(\mathcal{F}_p/\mathbb{Q}) \cong C_q \rtimes C_p$ non-abelian, and that its degree p subfield $\mathcal{K}_p$ is the first layer of the p-cyclotomic extension of $\mathbb{Q}$. Let $E/\mathbb{Q}$ be an elliptic curve, let f_E be the modular form attached to E and let $\mathbf{f}_E$ be the Hilbert modular form which is the base-change of f_E to the (totally real cyclic) extension $\mathcal{K}_p/\mathbb{Q}$. Assuming Conjecture 2.5.11, for any n such that $p^n \nmid q-1$ and primitive character ψ of $\mathrm{Gal}(\mathcal{F}_p\mathcal{K}_{p^n}/\mathcal{K}_p) \cong C_{qp^{n-1}}$, we have*

$$\mathrm{ord}_{s=1}\, L(\mathbf{f}_E, \psi, s) \equiv 0 \mod p,$$

where $\mathcal{K}_{p^n}$ is the n^{th} layer of the p-cyclotomic extension of $\mathbb{Q}$.

Question 5.2.4. *Our approach relies on elliptic curves. Are there similar phenomena for modular forms that do not correspond to elliptic curves?*

Example 5.2.5. *As a concrete example, take $p = 3$ and $q = 7$. For the degree 7 non-Galois extension $\mathcal{F}_1$ (see diagram above) take the field $\mathcal{F}_1 = \mathbb{Q}(\alpha)$ of discriminant $3^8 7^{12}$, where α is a root of $x^7 - 42x^5 - 70x^4 + 168x^3 + 126x^2 - 84x - 45$. As in the above discussion, take $\mathcal{K}_{3^n} = \mathbb{Q}(\zeta_{3^{n+1}})^+$ and set $\mathcal{F}_{3^n} = \mathcal{F}_1\mathcal{K}_{3^n}$, the n^{th} layer of the p-cyclotomic tower of $\mathcal{F}_1$. The field $\mathcal{F}_3$ is the Galois closure of $\mathcal{F}_1$ and $\mathrm{Gal}(\mathcal{F}_3/\mathbb{Q}) \cong C_7 \rtimes C_3$ non-abelian; this group is an analogue of a dihedral group with C_2 replaced by C_3.*

The group $\mathrm{Gal}(\mathcal{F}_3/\mathbb{Q}) \cong C_7 \rtimes C_3 = \langle a, b \,|\, a^7 = b^3 = id, bab^{-1} = a^2 \rangle$ has three 1-dimensional representations that come from the C_3-quotient, and two 3-dimensional irreducible representations τ_0, τ_0', which are induced from 1-dimensional characters ψ_0, ψ_0' of C_7; its character table is below.

$C_7 \rtimes C_3$	*id*	a	a^3	b	b^2
$\mathbb{1}$	1	1	1	1	1
χ_1	1	1	1	ζ_3	ζ_3^2
χ_2	1	1	1	ζ_3^2	ζ_3
τ_0	3	$\zeta_7 + \zeta_7^2 + \zeta_7^4$	$\zeta_7^3 + \zeta_7^5 + \zeta_7^6$	0	0
τ_0'	3	$\zeta_7^3 + \zeta_7^5 + \zeta_7^6$	$\zeta_7 + \zeta_7^2 + \zeta_7^4$	0	0

The irreducible representations of $\mathrm{Gal}(\mathcal{F}_{3^n}/\mathbb{Q}) \cong C_7 \rtimes C_{3^n}$ are the 1-dimensional representations lifted from the C_{3^n}-quotient, and 3-dimensional irreducibles that can all be written as $\tau = \tau_0 \otimes \chi$ or $\tau = \tau_0' \otimes \chi$ for some 1-dimensional χ; note that these can therefore also be expressed as $\tau = \mathrm{Ind}_{\mathcal{K}_3/\mathbb{Q}} \psi$, where $\psi = \psi_0 \otimes \mathrm{Res}\, \chi$ or $\psi_0' \otimes \mathrm{Res}\, \chi$ is 1-dimensional. The faithful ones are precisely the ones with χ of maximal order, equivalently with ψ of order $7 \times 3^{n-1}$.

Now let $E/\mathbb{Q}$ be an elliptic curve. The L-function in Theorem 5.2.1 can be expressed in several ways: if, say, $\tau = \tau_0 \otimes \chi = \mathrm{Ind}_{\mathcal{K}_3/\mathbb{Q}} \psi$ is 3-dimensional irreducible, then

$$L(E/\mathbb{Q}, \tau, s) = L(E/\mathbb{Q}, \tau_0 \otimes \chi, s) = L(E/\mathcal{K}_3, \psi, s) = L(\mathbf{f}_E, \psi, s),$$

where $\mathbf{f}_E$ is as in Corollary 5.2.3.

In this setting, our prediction is that the order of vanishing of this L-function is necessarily a multiple of 3, so long as τ does not factor through $C_7 \rtimes C_3$ (equivalently if the order of χ is at least 9). As we will explain in §5.3–5.4, the corresponding statement is provably true for the Mordell–Weil group $E(\mathcal{F}_{3^n})$, which is how we obtain the

prediction for L-functions and Selmer groups.

Finally, let us note that it is possible to make a prediction for analytic ranks that do not involve twisted L-functions, although it becomes a little cumbersome. Using the subfield lattice of $\mathcal{F}_{3^n}/\mathbb{Q}$ and inductivity of L-functions, one checks that

$$\frac{L(E/\mathcal{F}_{3^n},s)L(E/\mathcal{K}_{3^{n-1}},s)}{L(E/\mathcal{K}_{3^n},s)L(E/\mathcal{F}_{3^{n-1}},s)} = \prod_{\tau \text{ faithful}} L(E/\mathbb{Q},\tau,s)^3,$$

Observe that the faithful representations $\tau:\mathrm{Gal}(\mathcal{F}_{3^n}/\mathbb{Q}) \to \mathrm{GL}_3(\overline{\mathbb{Q}})$ have Galois conjugate images, since they are induced from Galois conjugate 1-dimensional ψ's. Thus, if we assume Conjecture 2.5.11 or Deligne's conjecture on Galois-equivariance of L-values [Del79, Conjecture 2.7ii], the orders of vanishing of their L-functions should all be equal, and hence the order of vanishing of the right-hand term in the above equation is a multiple of $3 \times 3 \times \frac{(7-1)(3^n-3^{n-1})}{3^2} = 4 \times 3^n$. In particular, if the L-values at $s=1$ are non-zero for $E/\mathcal{F}_{3^{n-1}}$ and $E/\mathcal{K}_{3^n}$ (and hence for $E/\mathcal{K}_{3^{n-1}}$), then the order of the zero of $L(E/\mathcal{F}_{3^n},s)$ must be a multiple of 4×3^n. More generally, the same technique yields the following result.

Corollary 5.2.6. *Let $\mathcal{F}/\mathbb{Q}$ be a Galois extension with $\mathrm{Gal}(\mathcal{F}/\mathbb{Q}) \cong C_q \rtimes C_{p^n}$ non-abelian, where the image of C_{p^n} in $\mathrm{Aut}\, C_q$ has order p^r and $p^n \nmid q-1$. Suppose $E/\mathbb{Q}$ is an elliptic curve such that $L(E/\mathcal{K},1) \neq 0$ for all proper subfields $\mathcal{K} \subsetneq \mathcal{F}$. If Conjecture 2.5.11 holds, then*

$$\mathrm{ord}_{s=1}\, L(E/\mathcal{F},s) \;\equiv\; 0 \mod p^{n-r}(p-1)(q-1).$$

Remark 5.2.7. *At present we do not have examples where the orders of vanishing of such L-functions are non-zero, as their conductors appear to be too large for any extensive numerical search. We also cannot guarantee a zero at $s=1$ by forcing the L-function to be essentially antisymmetric about that point: the twisting Artin representations τ (or $\tau \otimes \chi$) above are never self-dual, so the functional equation relates $L(E,\tau)$ to $L(E,\tau^*)$ and the root number ("sign") cannot be used to force a zero. The latter is a general feature of our approach, see Remark 5.3.7.*

Remark 5.2.8. *As will be clear from §5.3–5.4, Theorem 5.2.1 applies generally to abelian varieties over number fields, rather than elliptic curves over $\mathbb{Q}$.*

Remark 5.2.9. *The Galois representation $H^1_{\acute{e}t}(E,\mathbb{Q}_\ell)_{\mathbb{C}} \otimes \tau$ can be irreducible, so the multiplicity of the order of vanishing is not explained by a decomposition of the Galois representation. Moreover, the L-series is not the (formal) p^{th} power of another L-*

series. For example, if $G = C_7 \rtimes C_9$ and v is a prime of good reduction of E such that Frobenius at v is an element of order 7 in G, then the Euler factor at v is

$$\frac{1}{(1-\zeta_7\alpha p^{-s})(1-\zeta_7\beta p^{-s})(1-\zeta_7^2\alpha p^{-s})(1-\zeta_7^2\beta p^{-s})(1-\zeta_7^4\alpha p^{-s})(1-\zeta_7^4\beta p^{-s})},$$

which is visibly not a cube; here α and β are the Frobenius eigenvalues at v of E, and ζ_7 a suitable primitive 7-th root of unity.

Question 5.2.10. *For a self-dual Artin representation τ, the sign in the functional equation of $L(E,\tau,s)$ determines the parity of the order of vanishing at $s = 1$. The normalised L-function $\Lambda(E,\tau,s)$ has the "clean" completed functional equation*

$$\Lambda(E,\tau,s) = \pm\Lambda(E,\tau,2-s),$$

so, in particular, the Taylor series expansion around $s = 1$ has either only even terms or only odd terms. Is there any such effect for the L-functions in Theorem 5.2.1, i.e. can one normalise them so that the only non-zero coefficients in the Taylor expansion $\Lambda(E,\tau,s) = \sum_{k\geqslant 0} a_k(s-1)^k$ are the a_k with $p|k$?

5.3 Birch–Swinnerton-Dyer conjecture and the Schur index

Statements that concern the Birch–Swinnerton-Dyer conjecture usually suppose properties about a given L-function so as to ascertain information about the rank (e.g. Coates–Wiles, Gross–Zagier, Kolyvagin). Our approach is somewhat peculiar: we are traversing the opposite direction by using the Mordell–Weil group to derive a feature of the L-function. Recall the following generalisation of the Birch–Swinnerton-Dyer conjecture (cf. Conjecture 2.5.11): if τ is an Artin representation of a Galois extension of number fields $\mathcal{F}/\mathcal{K}$, then for all abelian varieties $A/\mathcal{K}$, we have

$$\operatorname{ord}_{s=1} L(A/\mathcal{K},\tau,s) = \langle A(\mathcal{F})_{\mathbb{C}},\tau\rangle.$$

The key observation is that since the Galois group acts on a $\mathbb{Z}$-lattice, $A(\mathcal{F})_{\mathbb{C}}$ is a rational representation. Therefore certain complex irreducible representations τ cannot appear with multiplicity 1 in $A(\mathcal{F})_{\mathbb{C}}$; this aspect is measured by the Schur index $m_{\mathbb{Q}}(\tau)$.

In contrast, the analogous property is not obvious (and unknown in general) for either the L-function of an abelian variety or the $\mathbb{Q}_\ell$-representation on the dual Selmer group $X_\ell(A/\mathcal{F})$.

Definition 5.3.1. *Let G be a finite group and $\mathscr{F}$ a subfield of $\mathbb{C}$. We say a complex representation τ of G is realisable over $\mathscr{F}$ if it is conjugate to a representation that factors as $G \to \mathrm{GL}_n(\mathscr{F}) \subset \mathrm{GL}_n(\mathbb{C})$ for some n. The Schur index $m_{\mathscr{F}}(\tau)$ is the maximal integer m such that for all representations σ of G that are realisable over $\mathscr{F}$, the multiplicity $\langle \tau, \sigma \rangle$ is a multiple of m.*

Remark 5.3.2. *If $\mathrm{Tr}\,\tau \subset \mathscr{F}$, then $m_{\mathscr{F}}(\tau) = 1$ if and only if τ is realisable over $\mathscr{F}$.*

Example 5.3.3. *Let $Q_8 = \langle i, j \mid i^4, i^2 = j^2, jij = i \rangle$ be the quaternion group and consider its 2-dimensional irreducible representation τ given by*

$$i \mapsto \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}, \qquad j \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Despite the fact that τ has real trace, it cannot be realised by matrices in $\mathrm{GL}_2(\mathbb{Q})$ which implies that its Schur index is not 1. However, there is a basis such that $\tau \oplus \tau$ is given by

$$i \mapsto \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}, \qquad j \mapsto \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$

which means that the Schur index of τ, $m_{\mathbb{Q}}(\tau)$, is 2 since we have realised $\tau \oplus \tau$ over $\mathbb{Q}$.

Remark 5.3.4. *Note that for any field $\mathscr{F}$, $m_{\mathscr{F}}(\tau) \leqslant \dim \tau$ as the regular representation is realisable over $\mathbb{Q}$. In fact $m_{\mathscr{F}}(\tau)$ always divides the dimension $\dim \tau$, see e.g. [Isa76, Corollary 10.2].*

Theorem 5.3.5. *Let $\mathcal{F}/\mathcal{K}$ be a Galois extension of number fields, and let τ be an irreducible Artin representation of $\mathrm{Gal}(\mathcal{F}/\mathcal{K})$. Then for all abelian varieties $A/\mathcal{K}$, the multiplicity of τ in $A(\mathcal{F})_{\mathbb{C}}$ is divisible by $m_{\mathbb{Q}}(\tau)$. In addition:*

i. If Conjecture 2.5.11 holds, then $\mathrm{ord}_{s=1} L(A/\mathcal{K}, \tau, s)$ is divisible by $m_{\mathbb{Q}}(\tau)$;

ii. If $Ш(A/\mathcal{F})[\ell^\infty]$ is finite for some prime ℓ, then $\langle X_\ell(A/\mathcal{F}), \tau \rangle$ is divisible by $m_{\mathbb{Q}}(\tau)$.

Proof. By construction, $A(\mathcal{F})_{\mathbb{C}}$ is realisable over $\mathbb{Q}$ hence $m_{\mathbb{Q}}(\tau)$ divides $\langle A(\mathcal{F})_{\mathbb{C}}, \tau \rangle$.

The L-function statement now follows directly from Conjecture 2.5.11. If $Ш(A/\mathcal{F})[\ell^\infty]$ is finite, then $X_\ell(A/\mathcal{F}) \cong A(\mathcal{F}) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$ as $\mathbb{Q}_\ell[\mathrm{Gal}(\mathcal{F}/\mathcal{K})]$-modules, from which the second part follows. □

Remark 5.3.6. *Without the finiteness assumption on* Ш*, the dual Selmer group $X_\ell(A/\mathcal{F})$ is not known to be a rational or even an orthogonal representation of the Galois group (although it is known to be self-dual, see [DD09b]). Thus, as the ℓ-adic Schur index $m_{\mathbb{Q}_\ell}(\tau)$ can be 1, there is no obvious representation-theoretic reason for the multiplicity of τ in $X_\ell(A/\mathcal{F})$ to be a multiple of $m_{\mathbb{Q}}(\tau)$; see Theorem 5.4.2 for an example of such a τ.*

Remark 5.3.7. *The reason for the restriction on the order of vanishing of the L-function is fairly well-understood for self-dual representations τ with Schur index 2 (for example the quaternion representation in Example 5.3.3). In this case the conjectural functional equation is of the form $L(A,\tau,s) = \pm L(A,\tau,2-s) \times (\Gamma$-factors and exponential$)$. So the parity of the order of vanishing at $s=1$ is determined by the sign $\pm$, which is given by the global root number $W(A,\tau)$ and known to be + whenever τ is symplectic and in many cases when τ is orthogonal with Schur index 2, see [Roh96, Proposition 2] and [Sab07, Theorem 0.1].*

It is tempting to use the sign in the functional equation to force a zero of the L-function for a representation τ with large Schur index $m = m_{\mathbb{Q}}(\tau)$. If Conjecture 2.5.11 is true, the order of vanishing is a fortiori at least m. Curiously enough, this is impossible to achieve: if $m > 2$, the representation τ cannot be self-dual by the Brauer–Speiser theorem. Thus the functional equation relates $L(A,\tau,s)$ to $L(A,\tau^*,2-s)$, and the root number cannot be used to force the L-function to vanish at $s=1$.

5.4 Schur indices in $C_q \rtimes C_{p^n}$

We now compute the Schur indices of representations of $C_q \rtimes C_{p^n}$ appearing in Theorem 5.2.1. We only prove that the Schur index is divisible by p without determining it exactly, so the bounds on orders of vanishing of L-functions that we have given may be suboptimal. For example, if τ is an irreducible faithful representation of $C_{19} \rtimes C_{3^4}$ (with the largest possible action), then $m_{\mathbb{Q}}(\tau) = 9$.

For a field $\mathscr{F}$ and representation τ, we let $\mathscr{F}(\tau)$ denote the finite abelian extension of $\mathscr{F}$ generated by the values of the trace of τ. We further let $N_{\mathscr{F}/\mathscr{K}}$ be the norm map for any field extension $\mathscr{F}/\mathscr{K}$.

Proposition 5.4.1. *Let p, q be distinct odd primes and $G = C_q \rtimes C_{p^n}$, where the image of C_{p^n} in $\operatorname{Aut} C_q$ has order p^r. Let τ be a complex irreducible representation of G. Write $X = C_q \times C_{p^{n-r}} \lhd G$.*

(i) If τ is unfaithful then τ is lifted either from C_{p^n} or from $C_q \rtimes C_{p^{n-1}}$.

(ii) If τ is faithful, then $\dim \tau = p^r$ and there is a faithful 1-dimensional representation of X such that $\tau = \operatorname{Ind}_X^G \psi$. Conversely, the induction of a faithful 1-dimensional representation ψ of X gives a faithful irreducible representation of G.

(iii) Every faithful irreducible representation τ of G may be written as $\tau_r \otimes \chi$ for some faithful irreducible representation τ_r of $C_q \rtimes C_{p^r}$ and faithful 1-dimensional representation χ of C_{p^n}.

(iv) If $\tau = \operatorname{Ind}_X^G \psi$ is faithful and $\mathscr{F} \subset \mathbb{C}$ is a field, then $\mathscr{F}(\psi) = \mathscr{F}(\zeta_{p^{n-r}}, \zeta_q)$ and $\mathscr{F}(\tau) = \mathscr{F}(\zeta_{p^{n-r}}, \sum_{t \in H} \zeta_q^t)$, where $H \leqslant (\mathbb{Z}/q\mathbb{Z})^\times$ is the subgroup of order p^r.

(v) If $\tau = \operatorname{Ind}_X^G \psi$ is faithful and $\mathscr{F} \subset \mathbb{C}$ is a field such that $[\mathscr{F}(\psi) : \mathscr{F}(\tau)] = p^r$, then the Schur index $m_{\mathscr{F}}(\tau) = 1$ if and only if $\zeta_{p^{n-r}}$ is in the image of $N_{\mathscr{F}(\psi)/\mathscr{F}(\tau)}$.

Proof. The group G has presentation $G = \langle a, b \mid a^q = b^{p^n} = \mathrm{id}, bab^{-1} = a^j \rangle$ where j has order p^r modulo q. The subgroup X is $\langle a, b^{p^r} \rangle$; it is the centraliser of C_q. For a representation ψ of X and a element $g \in G$ we write ${}^g\psi$ for the conjugate representation defined by ${}^g\psi(h) = \psi(ghg^{-1})$.

(i) The maximal quotients of G are C_{p^n} and (if $r < n$) $C_q \rtimes C_{p^{n-1}}$, so if τ is not faithful, it factors through one of these.

(ii) By [Ser77, Proposition 25], every faithful representation of G is necessarily induced from a 1-dimensional representation ψ of X; in particular $\dim \tau = p^r$. Moreover, since $\ker \psi$ is normal in G (as X is normal in G and $\ker \psi$ is characteristic in the cyclic group X), we have $\ker \psi \subseteq \ker \tau$, and hence ψ must be faithful.

Conversely, $h \mapsto b^k h b^{-k}$ are distinct automorphisms of X for $0 \leqslant k < p^r - 1$, so if ψ is a faithful 1-dimensional representation of X, then $\psi, {}^b\psi, \ldots, {}^{b^{p^r-1}}\psi$ are all distinct. Thus $\langle \tau, \tau \rangle = \langle \psi, \operatorname{Res}_X^G \operatorname{Ind}_X^G \psi \rangle = \langle \psi, \bigoplus_{0 \leqslant k < p^r} {}^{b^k}\psi \rangle = 1$ by Frobenius reciprocity and Mackey's formula, and so τ is irreducible. It is clearly faithful by (i).

(iii) Let $\tau = \operatorname{Ind}_X^G \psi$, for some faithful 1-dimensional ψ of order qp^{n-r}. We can rewrite this as $\psi = \psi_q \otimes \psi_{p^{n-r}}$ where ψ_m has order m. Now $\tau_r = \operatorname{Ind}_X^G \psi_q$ is the inflation of a faithful representation of $C_q \rtimes C_{p^r}$. Let χ be a 1-dimensional representation of G which factors through C_{p^n} such that $\operatorname{Res}_X^G \chi = \psi_{p^{n-r}}$. The push-pull formula shows

that $\tau = \tau_r \otimes \chi$, as claimed.

(iv) If τ is faithful, then by (ii) ψ is a faithful 1-dimensional representation of $X \cong C_{qp^{n-r}}$, hence $\mathscr{F}(\psi) = \mathscr{F}(\zeta_{qp^{n-r}})$. To compute $\mathscr{F}(\tau)$, it suffices to compute the induced character on the conjugacy classes of G which have nonempty intersection with X. Since $X \triangleleft G$, it follows that $\mathscr{F}(\tau) = \mathscr{F}(\mathrm{Res}^G_X \tau)$.

Note that b^{p^r} is central in G and τ is irreducible so $\tau(b^{p^r})$ must be scalar by Schur's lemma; as $\mathrm{Res}^G_X \tau$ contains ψ as a constituent, this scalar is multiplication-by-$\zeta_{p^{n-r}}$, hence $\zeta_{p^{n-r}} \in \mathscr{F}(\tau)$. For $a^x b^{p^r y} \in X$ we have $\mathrm{tr}\,\tau(a^x b^{p^r y}) = \zeta^y_{p^{n-r}} \mathrm{tr}\,\tau(a^x)$, so $\mathscr{F}(\tau)$ is generated over $\mathscr{F}$ by $\zeta_{p^{n-r}}$ and the traces $\mathrm{tr}\,\tau(a^x))$ for $1 \leqslant x \leqslant q$.

As in the proof in (ii), $\mathrm{Res}^G_X \tau = \bigoplus_{0 \leqslant k < p^r} {}^{b^k}\psi$, so $\mathrm{tr}\,\tau(a^x) = \sum_{t \in H} \zeta_q^{xt}$, where H is the unique index subgroup of order p^r contained in $(\mathbb{Z}/q\mathbb{Z})^\times$. Note that for any polynomial $f \in \mathbb{Q}[X]$, $f(\zeta_q)$ is $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugate to $f(\zeta_q^x)$ whenever $q \nmid x$, and hence $f(\zeta_q^x) \in \mathbb{Q}(f(\zeta_q))$ since $\mathbb{Q}(f(\zeta_q))/\mathbb{Q}$ is abelian. In particular, letting $f(X) = \sum_{t \in H} X^t$ (where we fix representatives for H), we see that $\sum_{t \in H} \zeta_q^{xt} \in \mathbb{Q}(\sum_{t \in H} \zeta_q^t)$ for all x. Hence $\mathscr{F}(\tau) = \mathscr{F}(\zeta_{p^{n-r}}, \sum_{t \in H} \zeta_q^t)$ as claimed.

(v) First note that X is normal, abelian and equal to its own centraliser, $X = C_G(X)$, as otherwise $b^k \in C_G(X)$ for some k with $p^r \nmid k$ which doesn't commute with a. Since by assumption the (abelian) extension $\mathscr{F}(\psi)/\mathscr{F}(\tau)$ has degree p^r, the representation ψ must have p^r distinct $\mathrm{Gal}(\mathscr{F}(\psi)/\mathscr{F}(\tau))$-conjugates, which then must be precisely the constituents of $\mathrm{Res}^G_X \tau$. Thus (G, X, τ) is an $\mathscr{F}$-triple, in the terminology of [Isa76, Definition 10.5]. Noting that $G = XC_{p^n}$, it then follows from [Isa76, Theorem 10.10] that $m_{\mathscr{F}}(\tau) = 1$ if and only if $\zeta_{p^{n-r}} \in N_{\mathscr{F}(\psi)/\mathscr{F}(\tau)}\mathscr{F}(\psi)$. □

Theorem 5.4.2. *Let p, q be distinct odd primes and $G = C_q \rtimes C_{p^n}$, where the image of C_{p^n} in $\mathrm{Aut}\, C_q$ has order p^r and $0 < r \leqslant n$. Let τ be a complex irreducible faithful representation of G. Then:*
(i) The Schur index $m_{\mathbb{Q}}(\tau) = p^s$ for some $0 < s \leqslant r$ if $p^n \nmid q-1$, and is 1 otherwise;
(ii) The Schur index $m_{\mathbb{Q}_q}(\tau) = m_{\mathbb{Q}}(\tau)$;
(iii) The Schur index $m_{\mathbb{Q}_\ell}(\tau) = 1$ for every prime $\ell \neq q$.

Proof. (iii) It is a general fact that if $\ell \nmid |G|$, then $m_{\mathbb{Q}_\ell}(\tau) = 1$; see for example [Gow75]. The Corollary in [Gow75] states more generally that if τ is irreducible modulo ℓ, then $m_{\mathbb{Q}_\ell}(\tau) = 1$; this will be our approach for the case $\ell = p$. To see that this holds, let σ be an irreducible constituent of τ modulo p. Now the eigenvalues of $\tau(a)$ (using the notation from the first paragraph of the proof of Proposition 5.4.1) are primitive q^{th} roots of unity, hence this also holds for σ. Let v be an eigenvector for $\sigma(a)$

with eigenvalue ζ. Then $\sigma(b^{-1})v$ is also an eigenvector for $\sigma(a)$ with eigenvalue ζ^j. As j has order p^r modulo q (note $q \neq p$), σ has p^r distinct eigenvalues, so $\dim \sigma = \dim \tau$ and hence τ is irreducible modulo p.

(ii) The global Schur index $m_{\mathbb{Q}}(\tau)$ is well known to equal the lowest common multiple of the local Schur indices $m_{\mathbb{Q}_v}(\tau)$ for all places v of $\mathbb{Q}$ (see for example [Olt09, Theorem 2.4]). Now τ is not self-dual (as G has odd order) so $m_{\mathbb{R}}(\tau) = 1$ hence the result is immediate from (iii).

(i) We prove instead the same statement for $m_{\mathbb{Q}_q}(\tau)$; the global statement for $m_{\mathbb{Q}}(\tau)$ then follows from (ii). Write $\tau = \mathrm{Ind}_X^G \psi$, as in Proposition 5.4.1(ii). By Proposition 5.4.1(iv), the extension $\mathbb{Q}_q(\psi)/\mathbb{Q}_q(\tau)$ is totally ramified of degree p^r, and so by (v) it suffices to check whether $\zeta_{p^{n-r}}$ is in the image of the norm map $N_{\mathbb{Q}_q(\psi)/\mathbb{Q}_q(\tau)}$.

By local class field theory, the subgroup of $\mathcal{O}^\times_{\mathbb{Q}_q(\tau)}$ consisting of norms from $\mathcal{O}^\times_{\mathbb{Q}_q(\psi)}$ has index p^r. Furthermore, as the extension is tame, $u \in \mathcal{O}^\times_{\mathbb{Q}_q(\tau)}$ is a norm if and only if its image $\bar{u}$ in the residue field $\mathbb{F}_{\mathbb{Q}_q(\tau)}$ of $\mathbb{Q}_q(\tau)$ is a norm from the residue field of $\mathbb{Q}_q(\psi)$; as the two residue fields are the same, this is equivalent to $\bar{u}$ being of the form $\bar{u} = x^{p^l}$ for some $x \in \mathbb{F}_{\mathbb{Q}_q(\tau)}$.

Thus we are reduced to checking whether $\mathbb{F}_{\mathbb{Q}_q(\tau)}$ contains a primitive p^n-th root of unity. Since $\mathbb{Q}_q(\tau)/\mathbb{Q}_q(\zeta_{p^{n-r}})$ is totally ramified (Proposition 5.4.1(iv)), by Hensel's Lemma this happens if and only if $\zeta_{p^n} \in \mathbb{Q}_q(\zeta_{p^{n-r}})$.

If $p^n | q-1$, then $\zeta_{p^n} \in \mathbb{Q}_q \subseteq \mathbb{Q}_q(\zeta_{p^{n-r}})$, and hence $m_{\mathbb{Q}_q}(\tau) = 1$.

Conversely, if $p^n \nmid q-1$, then $q \bmod p^n$ is a non-trivial element of p-power order (since $r > 0$ implies $q \equiv 1 \bmod p$) in $(\mathbb{Z}/p^n\mathbb{Z})^\times$. In particular, $\mathrm{Gal}(\mathbb{Q}_q(\zeta_{p^n})/\mathbb{Q}_q)$ contains an element of order p. All such elements fix $\zeta_{p^{n-r}}$, and consequently $\mathbb{Q}_q(\zeta_{p^{n-r}}) \neq \mathbb{Q}_q(\zeta_{p^n})$. It follows that $\zeta_{p^n} \notin \mathbb{Q}_q(\zeta_{p^{n-r}})$ and so $m_{\mathbb{Q}_q}(\tau) \neq 1$. It now follows from Remark 5.3.4 and Proposition 5.4.1(ii) that the Schur index is $m_{\mathbb{Q}_q}(\tau) = p^s$ for some $0 < s \leqslant r$. $\square$

Chapter 6

Frobenius elements in images of Galois representations

6.1 Introduction

Suppose $\mathcal{K}$ is a number field and $f \in \mathcal{K}[x]$ is an irreducible polynomial of degree n with splitting field $\mathcal{F}$. How can we determine the $\mathrm{Gal}(\mathcal{F}/K)$-conjugacy class of a Frobenius element above an unramified prime $\mathfrak{p}$, without explicitly constructing $\mathcal{F}$? This question is important for computation of L-functions (including twisted L-functions of abelian varieties) which necessarily require the image of Frobenius at every prime. If we consider the Galois action on the roots, we can identify $\mathrm{Gal}(\mathcal{F}/\mathcal{K})$ as a permutation group; the factorisation of f over the residue field of $\mathcal{K}$ at $\mathfrak{p}$ enables us to find the cycle type of Frobenius and hence we have it up to conjugacy in the symmetric group S_n.

Unfortunately, this is generally insufficient; the alternating group A_5 has two different conjugacy classes of the same cycle type. There is a method, known as *Serre's trick*, to obtain the extra information here, which we shall discuss momentarily. We note that Roberts [Rob04] has since extended this idea to all alternating groups before Dokchitser and Dokchitser [DD13] generalised this to any finite group (considered as a permutation group) by constructing suitable resolvents, akin to the alternating polynomial Serre used.

In number theory, Galois extensions also arise from Galois representations; here there is a natural linear action on the underlying vector space. All current applications of the algorithm of Dokchitser and Dokchitser are in fact to matrix groups [DDR16, Mas13, YZ15, Zen14] which motivates further study of this setting to improve the efficiency

of their current method. In this chapter, we present an algorithm for distinguishing conjugacy classes of Frobenius elements in matrix groups by taking advantage of this additional structure.

We do not give a complete answer for arbitrary matrix groups here but instead consider two separate cases. In the first case, we provide an approach (via the Weil pairing) which enables us to distinguish SL_n-conjugacy from GL_n-conjugacy; this is the matrix analogue of the S_n versus A_n situation. Our second case is when the Galois group in question is isomorphic to the quaternion group Q_8: we distinguish between the conjugacy classes of the order 4 elements by constructing suitable elements of the function field for each conjugacy class. In both cases, our Galois representations will arise from the $\mod l$ image of an elliptic curve to give context using the function field to produce our extra information. We also present a generalisation for the GL_n versus SL_n case to pinpoint precisely what structure of the elliptic curve we required to be able to do this for arbitrary representations.

We now return to the classical problem of separating A_5-conjugacy from S_5-conjugacy to illustrate the type of extra criterion we would like for the matrix setting.

6.1.1 Serre's trick

Let $\mathcal{F}$ be the splitting field of the irreducible polynomial $f = x^5 + 20x + 16 \in \mathbb{Q}[x]$ so $\mathrm{Gal}(\mathcal{F}/\mathbb{Q}) \cong A_5$. If f is reducible mod p for any unramified prime $p \nmid 10$, then the conjugacy class of a Frobenius element above p is completely determined.

However, f is irreducible mod 3 which implies that the Frobenius element above 3, Frob_3, is a 5-cycle but this is not sufficient as A_5 has two different conjugacy classes of 5-cycles. Let us order the roots of f in $\mathbb{C}$ as

$$\alpha_1 \approx -0.785,\ \alpha_2 \approx -1.27 + 1.55i,\ \alpha_3 = \overline{\alpha_2},\ \alpha_4 \approx 1.66 + 1.52i,\ \alpha_5 = \overline{\alpha_4}.$$

Then Frob_3 is $\mathrm{Gal}(\mathcal{F}/\mathbb{Q})$-conjugate to either $(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)$ or $(\alpha_1, \alpha_2, \alpha_3, \alpha_5, \alpha_4)$; we need to decide which. To distinguish between them we use *Serre's trick* (see [Buh78, p.53]) which uses a "square root of the discriminant".

Explicitly, we compute the value of

$$D_1 = \prod_{1 \leqslant i < j \leqslant 5} (\alpha_i - \alpha_j),$$

which corresponds to the alternating polynomial and under our ordering is equal to -32000. Note our approximations of the roots are sufficient as we know $D_1 \in \mathbb{Z}$ a priori since polynomials with alternating Galois groups necessarily have square discriminant.

We now do the same thing over the residue field but this time ordering the roots by the action of Frobenius and compute the same invariant D_2. If Frob_3 is conjugate to $(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)$, then we necessarily have that $D_1 \equiv D_2 \mod 3$ since conjugation in A_5 will not change the sign of D_1. If we had reordered our roots over $\mathbb{C}$ for the other class, then we would have obtained $-D_1$ originally so as $D_1 \not\equiv 0 \mod 3$, this criterion is also sufficient.

Indeed, we find that $D_2 = \prod_{1 \leqslant i < j \leqslant 5} (\beta_i - \beta_j) = 1$ where $\beta_i = \beta^{3^i}$ and β is any root of f in $\overline{\mathbb{F}}_3$. Hence Frob_3 is $\mathrm{Gal}(\mathcal{F}/\mathbb{Q})$-conjugate to $(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)$.

6.2 GL_n versus SL_n

We begin with our S_n versus A_n analogue: $\mathrm{GL}_n(\mathbb{F}_l)$ versus $\mathrm{SL}_n(\mathbb{F}_l)$. We illustrate our approach with the aid of elliptic curves, using the Weil pairing for our additional information. For the remainder of the section, we shall abbreviate $\mathrm{SL}_2(\mathbb{F}_l)$ and $\mathrm{GL}_2(\mathbb{F}_l)$ to SL_2 and GL_2 respectively and say the GL_2-conjugacy class of an element $\sigma \in \mathrm{SL}_2$ *splits* if its SL_2-conjugacy class is properly contained in its GL_2-conjugacy class.

Let $E/\mathcal{K}$ be an elliptic curve and fix a rational prime l. Then the action of $\mathrm{Gal}(\overline{\mathcal{K}}/\mathcal{K})$ on the group $E[l]$ of l-torsion points gives rise to the mod l Galois representation

$$\rho_{E,l} : \mathrm{Gal}(\overline{\mathcal{K}}/\mathcal{K}) \to \mathrm{GL}_2(\mathbb{F}_l),$$

which factors through $\mathrm{Gal}(\mathcal{F}/\mathcal{K})$, where $\mathcal{F} = \mathcal{K}(E[l])$ is the smallest extension of $\mathcal{K}$ over which all l-torsion points are defined.

Let $\mathfrak{p}$ be a prime of $\mathcal{K}$ which is unramified in $\mathcal{F}$ and does not divide the discriminant Δ_E of E (it suffices to assume $\mathfrak{p} \nmid l\Delta_E$; this is the assumption we will generally use). There are two standard pieces of information that we can acquire about the Frobenius element coming from its characteristic polynomial. Firstly, the determinant is equal to the absolute norm q of $\mathfrak{p}$. We can also ascertain its trace by examining the number of points on the reduced curve; the trace is equal to $q + 1 - |\tilde{E}(\mathbb{F}_\mathfrak{p})|$ where $\mathbb{F}_\mathfrak{p}$ is the residue field at $\mathfrak{p}$. This can be computed quite efficiently using either Schoof's

algorithm [Sch85] or the refined Schoof-Elkies-Atkin algorithm [Sch95].

Unfortunately, these two pieces of data do not always completely distinguish the conjugacy class, even in GL_2; for example the identity and $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ have the same trace and determinant. When it is difficult to establish the GL_2-class, we note that Duke and Tóth [DT02, Thm 2.1] give a method for determining this. Sutherland takes a different approach in [Sut16] to compute the entire Galois image by sampling various Frobenius elements; the need to determine their individual conjugacy classes also arises here.

Remark 6.2.1. *We shall suppose that* $\operatorname{Im}\rho_{E,l} = \mathrm{SL}_2$*, which implies that* $\zeta_l \in \mathcal{K}$ *and* $q \equiv 1 \bmod l$*. Recall that if* $\zeta_l \in \mathcal{K}$ *and* E *is an elliptic curve without complex multiplication, then* $\operatorname{Im}\rho_{E,l} = \mathrm{SL}_2$ *for all but finitely many primes* l *by Serre's open image theorem.*

We now give a further criterion to distinguish between two classes in SL_2 that are conjugate in GL_2. Let $\mathrm{GL}_2^{\square} := \{A \in \mathrm{GL}_2 \mid \det A \text{ is a square }\}$.

Theorem 6.2.2. *Let* $E/\mathcal{K}$ *be an elliptic curve such that* $\rho_{E,l}(\mathrm{Gal}(\overline{\mathcal{K}}/\mathcal{K})) = \mathrm{SL}_2$ *and* $\mathfrak{p}$ *be a prime of* $\mathcal{K}$ *of absolute norm* q *such that* $\mathfrak{p} \nmid l\Delta_E$*. Let* $\sigma \in \mathrm{SL}_2$ *be* GL_2*-conjugate to* $\rho_{E,l}(\mathrm{Frob}_{\mathfrak{p}})$ *and suppose that the* GL_2*-conjugacy class of* σ *splits in* SL_2*.*

Let $\tilde{E}$ *be the reduced curve at* $\mathfrak{p}$ *and suppose that* (Q_1, Q_2) *is an ordered basis of* $\tilde{E}[l]$ *such that the action of the Frobenius automorphism* $x \mapsto x^q$ *acts as* $\sigma \in \mathrm{SL}_2$ *on* $\tilde{E}[l]$ *with respect to* (Q_1, Q_2)*.*

Then $\rho_{E,l}(\mathrm{Frob}_{\mathfrak{p}})$*, written with respect to a global ordered basis* (P_1, P_2)*, is* SL_2*-conjugate to* σ *if and only if*

$$\langle P_1, P_2\rangle_l \bmod \mathfrak{p} \equiv \langle Q_1, Q_2\rangle_l^{k^2} \text{ for some } k \in \mathbb{Z},$$

where $\langle\ ,\ \rangle_l$ *denotes the Weil pairing.*

Proof. Write $\rho_{E,l}(\mathrm{Frob}_{\mathfrak{p}}) = \tau$ (with respect to P_1, P_2) and let $P_i' \in E[l]$ be such that $P_i' \bmod \mathfrak{p} = Q_i$ for $i = 1, 2$. First suppose that $\tau = \sigma$. If $P_i = P_i', i = 1, 2$, then the result trivially holds. Otherwise the possible ordered bases which give also give τ are in bijection with elements in the GL_2-centraliser $C_{\mathrm{GL}_2}(\sigma)$. By the orbit-stabiliser theorem, we can compute that the SL_2-centraliser of σ, $C_{\mathrm{SL}_2}(\sigma)$ has index $\frac{2}{l-1}$ in its GL_2-centraliser (as we impose that the SL_2-class splits) and moreover, $C_{\mathrm{GL}_2}(\sigma) = ZC_{\mathrm{SL}_2}(\sigma) \subset \mathrm{GL}_2^{\square}$, where Z is the centre of GL_2 which consists of scalar matrices.

Now suppose $\tau \neq \sigma$. By assumption, τ is GL_2-conjugate to σ so there exists $A \in \mathrm{GL}_2$

such that $\sigma = A^{-1}\tau A$. We claim that τ is SL_2-conjugate to σ if and only if $A \in \mathrm{SL}_2 C_{\mathrm{GL}_2}(\sigma) = \mathrm{GL}_2^{\square}$. Assume first that $A = A_1 A_2$ with $A_1 \in \mathrm{SL}_2$, $A_2 \in C_{\mathrm{GL}_2}(\sigma)$. Then $A_1^{-1}\tau A_1 = \sigma$ and we are done. Conversely, suppose σ, τ are SL_2-conjugate and write $\sigma = B^{-1}\tau B$ with $B \in \mathrm{SL}_2$. Then $B^{-1}A \in C_{\mathrm{GL}_2}(\sigma)$ which proves the claim.

Let α be the matrix that maps P_i' to P_i, $i = 1, 2$. Then $\langle P_1, P_2\rangle_l = \langle \alpha(P_1'), \alpha(P_2')\rangle_l = \langle P_1', P_2'\rangle_l^{\det \alpha} \bmod \mathfrak{p} \equiv \langle Q_1, Q_2\rangle^{\det \alpha}$. Then by the above argument, τ (with respect to P_1, P_2) is SL_2-conjugate to σ (with respect to Q_1, Q_2) if and only if $\alpha \in \mathrm{GL}_2^{\square}$ which completes the proof. □

Remark 6.2.3. *To discuss conjugacy questions about the image, it is necessary to fix a global basis as a reference point. In principle, one could then simply take the local basis to be the reduction of the global one; the* GL_2*-conjugacy class then suffices to determine the* SL_2 *class.*

However, determining a global basis precisely enough is computationally expensive for large l *so this is far from ideal. In practice, we use the lattice interpretation of the elliptic curve; this enables us to compute a global basis as points in* $E(\mathbb{C})$ *(together with their Weil pairing) with minimal effort. This approach simplifies the global calculation but prevents us from computing their images in the residue field easily, which is where we then apply our theorem to distinguish conjugacy.*

We do not actually need the image to be SL_2 to apply the above theorem. However, $\mathcal{K}$ may not contain the relevant roots of unity so to combat this we should consider the minimal polynomials.

Let $m_{\mathcal{K}}(\alpha)$ denote the minimal polynomial of α over $\mathcal{K}$, for any field $\mathcal{K}$ and algebraic number α.

Theorem 6.2.4. *Let* $E/\mathcal{K}$ *be an elliptic curve and let* $\rho_{E,l}(\mathrm{Gal}(\overline{\mathcal{K}}/\mathcal{K})) = G \subset \mathrm{GL}_2$. *Let* $\mathfrak{p}$ *be a prime of norm* q *such that* $\mathfrak{p} \nmid l\Delta_E$ *and* $q \equiv 1 \bmod l$. *Let* $\sigma \in \mathrm{SL}_2$ *be* GL_2*-conjugate to* $\rho_{E,l}(\mathrm{Frob}_{\mathfrak{p}})$ *and suppose that the* G*-conjugacy class of* σ *is equal to the intersection of* G *with its* SL_2*-conjugacy class.*

Let $\tilde{E}$ *be the reduced curve at* $\mathfrak{p}$ *and suppose that* (Q_1, Q_2) *is an ordered basis of* $\tilde{E}[l]$ *such that the action of the Frobenius automorphism* $x \mapsto x^q$ *acts as* σ *on* $\tilde{E}[l]$ *with respect to* (Q_1, Q_2).

Then $\rho_{E,l}(\mathrm{Frob}_{\mathfrak{p}})$*, written with respect to a global ordered basis* (P_1, P_2)*, is* G*-conjugate*

to σ if and only if

$$m_{\mathbb{F}_\mathfrak{p}}(\langle Q_1, Q_2\rangle_l^{k^2}) \text{ divides } m_\mathcal{K}(\langle P_1, P_2\rangle_l) \bmod \mathfrak{p}$$

for some $k \in \mathbb{Z}$, where $\mathbb{F}_\mathfrak{p}$ is the residue field of $\mathcal{K}$ at $\mathfrak{p}$.

Proof. By the assumption on G, $\rho_{E,l}(\mathrm{Frob}_\mathfrak{p})$ is G-conjugate to σ if and only if it is SL_2-conjugate to σ, with respect to the same global ordered basis (P_1, P_2). Let $\mathcal{L} = \mathcal{K}(\zeta_l)$. Then for any prime $\mathfrak{P}$ of $\mathcal{L}$ above $\mathfrak{p}$, we have that $\rho_{E,l}(\mathrm{Frob}_\mathfrak{P})$, with respect to (P_1, P_2), is G-conjugate to σ if and only if $\langle Q_1, Q_2\rangle_l^{k^2} \equiv \langle P_1, P_2\rangle_l \bmod \mathfrak{P}$ for some $k \in \mathbb{Z}$ by Theorem 6.2.2.

As $q \equiv 1 \bmod l$, $\mathfrak{p}$ splits completely in L hence $\mathrm{Frob}_\mathfrak{P} = \mathrm{Frob}_\mathfrak{p}$. Moreover, $m_{\mathbb{F}_\mathfrak{p}} := m_{\mathbb{F}_\mathfrak{p}}(\langle Q_1, Q_2\rangle_l^{k^2})$ is linear and $m_\mathcal{K} := m_\mathcal{K}(\langle P_1, P_2\rangle_l) = \prod_{g \in \mathrm{Gal}(\mathcal{L}/\mathcal{K})} (x - g(\langle P_1, P_2\rangle_l))$. It remains to show $m_{\mathbb{F}_\mathfrak{p}}$ divides $m_\mathcal{K} \bmod \mathfrak{p}$ if and only if $\langle Q_1, Q_2\rangle_l^{k^2} \equiv \langle P_1, P_2\rangle_l \bmod \mathfrak{P}$ for some choice of $\mathfrak{P}|\mathfrak{p}$.

Suppose $\langle Q_1, Q_2\rangle_l^{k^2} \equiv \langle P_1, P_2\rangle_l \bmod \mathfrak{P}$. As $m_{\mathbb{F}_\mathfrak{p}}$ is linear, we have divisibility $\bmod \mathfrak{P} \cap \mathcal{K} = \mathfrak{p}$. Conversely, fix $\mathfrak{P}$ and suppose $m_{\mathbb{F}_\mathfrak{p}}$ divides $m_\mathcal{K} \bmod \mathfrak{p}$. Then $\langle Q_1, Q_2\rangle_l^{k^2} \equiv g(\langle P_1, P_2\rangle_l) \bmod \mathfrak{P}$ for some $g \in \mathrm{Gal}(\mathcal{L}/\mathcal{K})$ and hence $\langle Q_1, Q_2\rangle_l^{k^2} \equiv \langle P_1, P_2\rangle_l \bmod g^{-1}(\mathfrak{P})$. □

Example 6.2.5. *Let $E/\mathbb{Q}(\zeta_3)$ be the elliptic curve $y^2 = x^3 + x + 1$ (Cremona label 496a1), where $\zeta_3 = e^{2\pi i/3}$. The image of the mod 3 representation of $E/\mathbb{Q}(\zeta_3)$ is isomorphic to $\mathrm{SL}_2(\mathbb{F}_3)$. Let $\mathfrak{p} = (13, \zeta_3 - 3)$ be a prime of $\mathbb{Q}(\zeta_3)$. We shall compute the SL_2-conjugacy class of $\rho_{E,3}(\mathrm{Frob}_\mathfrak{p})$.*

Choose a global basis $P_1 = (\alpha_1, \beta_1), P_2 = (\overline{\alpha_1}, \overline{\beta_1}) \in E(\mathbb{C})$, where $\alpha_1 \approx 0.571 + 1.754i, \beta_1 \approx 0.984 + 2.761i$ and observe that $\langle P_1, P_2\rangle_3 = \zeta_3$.

Now the reduced curve $\tilde{E}$ has 18 points so the trace of Frobenius is $2 \bmod 3$, hence the image of Frobenius (with respect to (P_1, P_2)) is SL_2-conjugate to $\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$ for some $n \in \{0, 1, 2\}$. These all define distinct SL_2-conjugacy classes, with the non-identity elements being GL_2-conjugate.

A quick check shows that $\tilde{E}(\mathbb{F}_{13})[3] \neq 9$ hence $n \neq 0$ so $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ is GL_2-conjugate to $\rho_{E,3}(\mathrm{Frob}_\mathfrak{p})$.

Now $\tilde{E}[3]$ is defined over the cubic extension $\mathbb{F}_{13}[\alpha]$, where α has minimal polynomial $x^3 + 2x - 2$. We compute that $Q_1 = (10, 6)$, $Q_2 = (8\alpha^2 - \alpha + 3, 7\alpha^2 + 4\alpha - 1)$ is a basis of $\tilde{E}[3]$ such that the Frobenius automorphism acts as $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ here.

The criterion we have in this case is equivalent to checking whether

$$\langle P_1, P_2 \rangle_3 \equiv \langle Q_1, Q_2 \rangle_3 \bmod \mathfrak{p}.$$

A quick calculation shows that $\langle Q_1, Q_2 \rangle_3 = 3$ *so* $\rho_{E,3}(\mathrm{Frob}_\mathfrak{p})$ *is* SL_2*-conjugate to* $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ *with respect to* (P_1, P_2).

Example 6.2.6. *Consider the elliptic curve* $y^2 + y = x^3 - x^2$ *(Cremona label 11a3) defined over* $\mathbb{Q}(\sqrt{5})$. *The mod* 5 *image*[1] *is isomorphic to* D_{10}*, the dihedral group of order 10 generated by* $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ *and* $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 4 \end{smallmatrix}\right)$. *This is not contained in* $\mathrm{SL}_2(\mathbb{F}_5)$ *but the order* 5 *elements satisfy the conditions of Theorem 6.2.4.*

Let $\mathfrak{p} = (\frac{1+5\sqrt{5}}{2})$ *be a prime of* $\mathbb{Q}(\sqrt{5})$ *above* 31. *Choose the ordered global basis* $P_1 \approx (1.69 - 1.54i, -1.27 + 2.83i), P_2 = (1, -1)$ *so* $\langle P_1, P_2 \rangle_5 = e^{2\pi i/5}$. *This is not an element of* $\mathbb{Q}(\sqrt{5})$ *so we instead take its minimal polynomial* $m_{\mathbb{Q}(\sqrt{5})}(e^{2\pi i/5}) = x^2 + \frac{1}{2}(1+\sqrt{5})x + 1$.

One can check that $\mathrm{Frob}_\mathfrak{p}$ *has order* 5 *using the group structure of the reduced curve and so is conjugate to either* $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ *or* $\left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right)$ *under the ordered basis* (P_1, P_2).

Let $Q_1 = (1, -1), Q_2 = (26\alpha^3 + 8\alpha^2 + 23\alpha + 12, 16\alpha^4 + 17\alpha^3 + 29\alpha^2 + 17\alpha + 2)$*, where* α *has minimal polynomial* $x^5 + 7x + 28$ *over* $\mathbb{F}_{31}$. *Then the Frobenius automorphism acts on* $\tilde{E}[5]$ *as* $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ *with respect to the ordered basis* (Q_1, Q_2).

We compute that $\langle Q_1, Q_2 \rangle_5 = 8$. *Now* $m_{\mathbb{Q}(\sqrt{5})}(e^{2\pi i/5}) \equiv x^2 + 13x + 1 \bmod \mathfrak{p}$ *which does not have* 8 *as a root so* $\mathrm{Frob}_\mathfrak{p}$ *cannot be conjugate to* $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. *Redoing the calculation with* $\left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right)$*, (where we take the basis* $(Q_1, Q_1 + 2Q_2)$*), the Weil pairing is* 2 *which is now a root of* $m_{\mathbb{Q}(\sqrt{5})}(e^{2\pi i/5}) \bmod \mathfrak{p}$. *Hence* $\mathrm{Frob}_\mathfrak{p}$ *is* D_{10}*-conjugate to* $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ *with respect to the basis* (P_1, P_2).

Remark 6.2.7. *We ran our method against the current algorithm of Dokchitser and Dokchitser in Magma [BCP97]. Their algorithm is not yet implemented over number fields so we only ran ours for rational primes which were completely split in the base field so the Frobenius element is unchanged. In addition, the bulk of the computation in their method consists of constructing a polynomial for each conjugacy class first. For a fairer comparison, we chose to time the results to determine the Frobenius elements at 1000 suitable rational primes in the mod* $3, 5, 7$ *and* 11 *representations of the elliptic curve* $y^2 = x^3 + x + 1$*; the computation was run on a machine with an AMD Opteron(tm) Processor 6174 and a speed of 2200MHz. We tabulate our results below.*

[1] The mod 5 image was obtained from [Col17, elliptic curve 11.a3] at `http://www.lmfdb.org/EllipticCurve/Q/11/a/3`, using data computed via methods in [Sut16].

l	*Weil pairing method*	*Dokchitsers' method*
3	5.7 *seconds*	0.5 *seconds*
5	25.7 *seconds*	11.4 *seconds*
7	88.7 *seconds*	1032.3 *seconds*
11	373.4 *seconds*	> 7 *days*

The final thing we wish to address is how beneficial elliptic curves were here as to the feasibility of this method for Galois representations arising from other types of objects. We can also do this for larger dimensional vector spaces, so we will incorporate this into our theorem.

We first recall a construction which generalises the precise properties of the Weil pairing that we want. Let $V/\mathbb{F}_l$ be a vector space of dimension n. Then the n^{th} exterior power $\Lambda^n V^*$ is a one dimensional vector space of alternating multilinear forms, such that for any nonzero $T \in \Lambda^n V^*$ we have

i. $T(v_1, \cdots, v_n) = 0$ if and only if $\{v_1, \cdots, v_n\}$ are linearly dependent,

ii. $T(Av_1, \cdots, Av_n) = \det(A)T(v_1, \cdots, v_n)$ for all matrices $A \in \mathrm{GL}_n(\mathbb{F}_l)$.

In the case of the Weil pairing, we identified the image $\mathbb{F}_l$ with the l^{th} roots of unity and shall do so again in our final theorem. For a field $\mathcal{K}$, we let $\mu_l(\mathcal{K})$ denote the l^{th} roots of unity in $\mathcal{K}$.

Theorem 6.2.8. *Let $\mathcal{F}/\mathcal{K}$ be a Galois extension of number fields and let ρ be a Galois representation such that $\rho : \mathrm{Gal}(\mathcal{F}/\mathcal{K}) \to \mathrm{SL}_n(\mathbb{F}_l)$ is an isomorphism for some rational prime l and positive integer n. Let $\mathfrak{p}$ be a prime of $\mathcal{K}$ which is unramified in $\mathcal{F}$ and $\mathfrak{P}$ a prime of $\mathcal{F}$ above $\mathfrak{p}$ with corresponding residue fields $\mathbb{F}_\mathfrak{p}$ and $\mathbb{F}_\mathfrak{P}$. Write $G = \mathrm{Gal}(\mathcal{F}/\mathcal{K})$ and $\overline{G} = \mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$, where we identify the latter with the decomposition subgroup.*

Let $V, \overline{V}$ be two $\mathbb{F}_l$-vector spaces of dimension n. Suppose V (respectively $\overline{V}$) has a faithful action of G (respectively $\overline{G}$) and there exists an isomorphism $\theta : V \to \overline{V}$ such that $\theta\overline{g} = \overline{g}\theta$ for all $\overline{g} \in \overline{G}$. Furthermore, suppose that there are nonzero alternating multilinear forms $T_\mathcal{K} \in \Lambda^n V^*$ and $T_{\mathbb{F}_\mathfrak{p}} \in \Lambda^n \overline{V}^*$ such that the diagram

$$\begin{array}{ccc} V^n & \xrightarrow{T_\mathcal{K}} & \mu_l(\mathcal{K}) \\ \downarrow{\scriptstyle \tilde{\theta}} & & \downarrow{\scriptstyle \bmod \mathfrak{p}} \\ \overline{V}^n & \xrightarrow{T_{\mathbb{F}_\mathfrak{p}}} & \mu_l(\mathbb{F}_\mathfrak{p}) \end{array}$$

commutes, where $\tilde{\theta}(v_1, \cdots, v_n) := (\theta(v_1), \cdots, \theta(v_n))$.

Suppose the $\mathrm{GL}_n(\mathbb{F}_l)$*-conjugacy class of* $\rho(\mathrm{Frob}_\mathfrak{p})$ *splits into* m *classes in* $\mathrm{SL}_n(\mathbb{F}_l)$ *and let* $H \subset \mathbb{F}_l^\times$ *be the unique subgroup such that* $[\mathbb{F}_l^\times : H] = m$*. Suppose* $\sigma \in \mathrm{SL}_n(\mathbb{F}_l)$ *is* $\mathrm{GL}_n(\mathbb{F}_l)$*-conjugate to* $\rho(\mathrm{Frob}_\mathfrak{p})$ *and let* $\overline{B}$ *be an ordered basis of* $\overline{V}$ *such that the Frobenius automorphism acts as* σ *on* $\overline{V}$ *with respect to* $\overline{B}$*. Then* $\rho(\mathrm{Frob}_\mathfrak{p})$*, written with respect to a global ordered basis* B*, is* $\mathrm{SL}_n(\mathbb{F}_l)$*-conjugate to* σ *if and only if*

$$T_\mathcal{K}(B) \mod \mathfrak{p} \equiv T_{\mathbb{F}_\mathfrak{p}}(\overline{B})^h \qquad \textit{for some } h \in H.$$

Proof. Let $B' = \tilde{\theta}^{-1}(\overline{B})$ and suppose first that $\tau = \sigma, B = B'$. Then $T_\mathcal{K}(B) = T_\mathcal{K}(\tilde{\theta}^{-1}(\overline{B}))$ and the result follows from the commutativity of the diagram.

Otherwise, we mimic the proof of Theorem 6.2.2, where $[C_{\mathrm{GL}_n(\mathbb{F}_l)}(\sigma) : C_{\mathrm{SL}_n(\mathbb{F}_l)}(\sigma)] = \frac{m}{l-1}$. We have that if $A \in \mathrm{GL}_n(\mathbb{F}_l)$ is such that $\sigma = A^{-1}\tau A$, then σ, τ are $\mathrm{SL}_n(\mathbb{F}_l)$-conjugate if and only if $A \in \mathrm{SL}_n(\mathbb{F}_l)C_{\mathrm{GL}_n(\mathbb{F}_l)}(\sigma)$ and there is an isomorphism

$$\frac{\mathrm{GL}_n(\mathbb{F}_l)}{\mathrm{SL}_n(\mathbb{F}_l)C_{\mathrm{GL}_n(\mathbb{F}_l)}(\sigma)} \cong \mathbb{F}_l^\times / H$$

via the determinant map and hence $\det C_{\mathrm{GL}_n(\mathbb{F}_l)}(\sigma) = H$. Therefore

$$C_{\mathrm{GL}_n(\mathbb{F}_l)}(\sigma) \subset \mathrm{GL}_n^H(\mathbb{F}_l) = \{A \in \mathrm{GL}_n(\mathbb{F}_l) |\ \det A \in H\} = \mathrm{SL}_n(\mathbb{F}_l)C_{\mathrm{GL}_n(\mathbb{F}_l)}(\sigma)$$

and the result now follows from the fact that $T_\mathcal{K}(\alpha B) = T_\mathcal{K}(B)^{\det \alpha}$ for any $\alpha \in \mathrm{GL}_n(\mathbb{F}_l)$. □

6.3 The quaternion group

Now we consider another method to distinguish conjugacy classes when $\mathrm{Im}\,\rho_{E,l}$ is isomorphic to the quaternion group $Q_8 = \langle i, j \,|\, i^4, i^2 = j^2, jij = i\rangle$. The classes we wish to distinguish between have representatives i, j and $k = ij$. We will not give an algorithm to distinguish Frobenius elements in the general case, but focus one particular case. We summarise the main result of this section below.

Theorem 6.3.1 (=Theorem 6.3.10)**.** *Let* $E/\mathcal{K}$ *be an elliptic curve over a number field* $\mathcal{K}$ *and suppose that* $\mathrm{Im}\,\rho_{E,3} \cong Q_8$*. Fix a basis* P, Q *of* $E[3]$ *and let* $i, j, k \in \mathrm{Aut}(E[3])$ *be matrices corresponding to non-conjugate order* 4 *elements of* $\mathrm{Gal}(\mathcal{K}(E[3])/\mathcal{K})$ *with respect to this basis. Let* $\mathfrak{p}$ *be a prime of* $\mathcal{K}$ *such that* $\mathfrak{p} \nmid 3\Delta_E$ *and* $\rho_{E,3}(\mathrm{Frob}_\mathfrak{p})$ *is* $\mathrm{GL}_2(\mathbb{F}_3)$*-conjugate to* i*.*

Then there exists functions $F_i, F_j, F_k \in \mathcal{K}(E)$ (to be constructed later; see Proposition 6.3.16 for their general form) and a function $G \in \frac{\mathcal{O}_\mathcal{K}}{\mathfrak{p}}(\tilde{E})$ (also constructed later; here $\tilde{E}$ is the reduction of E at $\mathfrak{p}$) such that if F_i, F_j, F_k are distinct modulo $\mathfrak{p}$, then

i. $\rho_{E,3}(\mathrm{Frob}_\mathfrak{p})$ *is* $\mathrm{Gal}(\mathcal{K}(E[3])/\mathcal{K})$*-conjugate to* i *if and only if* $F_i \equiv G \mod \mathfrak{p}$*;*

ii. $\rho_{E,3}(\mathrm{Frob}_\mathfrak{p})$ *is* $\mathrm{Gal}(\mathcal{K}(E[3])/\mathcal{K})$*-conjugate to* j *if and only if* $F_j \equiv G \mod \mathfrak{p}$*;*

iii. $\rho_{E,3}(\mathrm{Frob}_\mathfrak{p})$ *is* $\mathrm{Gal}(\mathcal{K}(E[3])/\mathcal{K})$*-conjugate to* k *if and only if* $F_k \equiv G \mod \mathfrak{p}$*.*

Before we can start, we first need to realise Q_8 as a Galois representation of an elliptic curve which we now do.

Lemma 6.3.2. *Let* $i = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$, $j = \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_3)$*. Then the subgroup* $\langle i, j \rangle$ *is the unique subgroup of* $\mathrm{GL}_2(\mathbb{F}_3)$ *isomorphic to* Q_8*.*

Since this is unique, it is characteristic with quotient isomorphic to S_3. When the mod 3 image is surjective , we would like to determine precisely what this S_3 extension is. Note that this subgroup is contained in $\mathrm{SL}_2(\mathbb{F}_3)$ so the extension should contain the cube roots of unity.

Lemma 6.3.3. *Let $E/\mathcal{K}$ be an elliptic curve over a characteristic 0 field $\mathcal{K}$ such that the mod 3 representation is surjective. Then* $\mathrm{Gal}(\mathcal{K}(E[3])/\mathcal{K}(\zeta_3, \Delta_E^{1/3})) \cong Q_8$*, where Δ_E is the discriminant of E.*

Proof. Recall that for any elliptic curve $E/\mathcal{K}$, the Weil pairing implies that $\mathrm{Im}\,\rho_{E,3} \subset \mathrm{SL}_2(\mathbb{F}_3)$ if and only if $\zeta_3 \in \mathcal{K}$. We claim that the polynomial $x^3 - \Delta_E$ splits over $\mathcal{K}(E[3])$; this would then cut out the unique index 3 subgroup of $\mathrm{Gal}(\mathcal{K}(E[3])/\mathcal{K}(\zeta_3)) \cong \mathrm{SL}_2(\mathbb{F}_3)$, which is isomorphic to Q_8.

To see the claim, we shall suppose for simplicity that $E/\mathcal{K}$ is given in the form $y^2 = x^3 + Ax + B$. Then the 3-division polynomial has as its roots the x-coordinates of $E[3]$ and is given by $x^4 + 2Ax^2 + 4Bx - \frac{1}{3}A^2$.

The resolvent cubic[2] of this is $x^3 - 2Ax^2 + \frac{4}{3}A^2x - \frac{8}{3}A^3 - 16B^2$ which by construction also splits over $\mathcal{K}(E[3])$. Using the substitution $x = t + \frac{2}{3}A$, we obtain the depressed cubic $t^3 + \frac{-64}{27}A^3 - 16B^2 = t^3 + \frac{1}{27}\Delta_E$, where $\Delta_E = -16(4A^3 + 27B^2)$ is the discriminant of E. □

[2]If $\alpha, \beta, \gamma, \delta$ are roots of a quartic polynomial f, then its resolvent cubic has roots $\alpha\beta + \gamma\delta, \alpha\gamma + \beta\delta$ and $\alpha\delta + \beta\gamma$.

Remark 6.3.4. *The discriminant of an elliptic curve is a priori model-dependent which is unfortunate. One can prove directly that the splitting field of $x^3 - \Delta_E$ is independent of model. A simpler approach is to use the j-invariant which is independent of the model. Observe that the j-invariant is given by $j = \frac{(-48A)^3}{\Delta_E}$; in particular the discriminant is a cube if and only if the j-invariant is a cube.*

Now that we have realised Q_8 as a Galois representation, we return to our question of distinguishing conjugacy classes. The classes of interest here have representatives i, j and $k = ij = \left(\begin{smallmatrix} 1 & 2 \\ 2 & 2 \end{smallmatrix}\right)$ which are all $\mathrm{GL}_2(\mathbb{F}_3)$-conjugate. Fix a basis P, Q for $E[3]$ and observe that the orbits of the points of order 3, $E[3] \setminus \{\mathcal{O}\}$, under i, j and k are

$$\begin{aligned} i: &\quad \{P, 2P, Q, 2Q\}, \{P+Q, 2P+Q, 2P+2Q, P+2Q\}; \\ j: &\quad \{P, 2P+2Q, 2P, P+Q\}, \{Q, 2P+Q, 2Q, P+2Q\}; \\ k: &\quad \{P, P+2Q, 2P, 2P+Q\}, \{Q, 2P+2Q, 2Q, P+Q\}. \end{aligned}$$

We can use these orbits to construct the following degree 0 Weil divisors:

$$\begin{aligned} D_i &= (P)+(Q)+(2P)+(2Q)-(P+Q)-(2P+Q)-(2P+2Q)-(P+2Q); \\ D_j &= (P)+(2P+2Q)+(2P)+(P+Q)-(Q)-(2P+Q)-(2Q)-(P+2Q); \\ D_k &= (P)+(P+2Q)+(2P)+(2P+Q)-(Q)-(2P+2Q)-(2Q)-(P+Q). \end{aligned}$$

Moreover, by considering the image of these divisors under the Abel–Jacobi map, these are principal divisors, so we let $f_i, f_j, f_k \in \mathcal{K}(E[3])(E)^\times$ be the functions corresponding to these divisors, where we normalise by making them monic so that our functions are uniquely defined.

Definition 6.3.5. *Let $E/\mathcal{L}$ be an elliptic curve with identity $\mathcal{O}$. Then a function $f \in \mathcal{L}(E)^\times$ is* monic *if* $\left(\left(\frac{x}{y}\right)^{-\mathrm{ord}_{\mathcal{O}}(f)} f\right)(\mathcal{O}) = 1$.

We would like to be able to compare these functions directly to distinguish between conjugacy classes. A priori though, the coefficient field is $\mathcal{K}(E[3])$; to enable us to change our field of definition, we use the following lemma.

Lemma 6.3.6. *Let $E/\mathcal{K}$ be an elliptic curve, $\mathcal{L}/\mathcal{K}$ a finite Galois extension, $f \in \mathcal{L}(E)$ such that its divisor is stable under the action of $\mathrm{Gal}(\mathcal{L}/\mathcal{K})$. Then there exists $\lambda \in \mathcal{L}$, $f' \in \mathcal{K}(E)$ such that $f = \lambda f'$. In particular, if f is monic, then $f \in \mathcal{K}(E)$.*

Proof. This is a simple application of Hilbert's Theorem 90; see for example [Cas91, p.107]. □

Remark 6.3.7. *The monic assumption is required since the divisor of the constant function $f = \sqrt{2} \in \mathbb{Q}(\sqrt{2})(E)$ is zero which is trivially stable under $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ for any elliptic curve $E/\mathbb{Q}$. If we force it to be monic however, we get $f = 1$ which now lives in $\mathbb{Q}(E)$.*

Hence our monic assumption will allow us to directly compare them if the divisors are stable under the action of Q_8; unfortunately this isn't true since $j(D_i) \neq D_i$. However, we note that D_i is stable under i but $j(D_i) = k(D_i) = -D_i$ and likewise for D_j, D_k. The only operation on divisors we have is addition but this is unsuitable as this would return the zero divisor in each case.

Instead we observe that the monic function with divisor $-D_i$ is simply $\frac{1}{f_i}$ so we choose to sum them and define $F_i = f_i + \frac{1}{f_i}$ (multiplication of functions corresponds to addition of divisors). Now as f_i is stable under i and $j(f_i) = \frac{1}{f_i}$, F_i is stable under the full Q_8 action and hence so is its divisor. As we have assumed f_i was monic, the above lemma tells us that $F_i \in \mathcal{K}(E)$.

We similarly define $F_j = f_j + \frac{1}{f_j}$ and $F_k = f_k + \frac{1}{f_k}$; these are the functions we work with.

Remark 6.3.8. *In our original construction of the divisors D_i, D_j, D_k, we had to place an order on our orbits. However our construction of F_i, F_j, F_k now makes this independent of the order and only on the Galois elements i, j, k which is what we want.*

Lemma 6.3.9. *Let $E/\mathcal{K} : y^2 = x^3 + Ax + B$ be an elliptic curve and let P, Q be a basis for $E[3]$ and let $i = \left(\begin{smallmatrix} 0 & 2 \\ 1 & 0 \end{smallmatrix}\right), j = \left(\begin{smallmatrix} 2 & 2 \\ 2 & 1 \end{smallmatrix}\right), k = ij \in \mathrm{Aut}(E[3])$ with respect to this basis. Then*

$$\begin{aligned} F_i &= \frac{(x - x_P)^2(x - x_Q)^2 + (x - x_{P+Q})^2(x - x_{2P+Q})^2}{\psi_3}, \\ F_j &= \frac{(x - x_P)^2(x - x_{P+Q})^2 + (x - x_Q)^2(x - x_{2P+Q})^2}{\psi_3}, \\ F_k &= \frac{(x - x_P)^2(x - x_{P+2Q})^2 + (x - x_Q)^2(x - x_{P+Q})^2}{\psi_3}, \end{aligned}$$

where $\psi_3 = x^4 + 2Ax^2 + 4Bx - \frac{1}{3}A^2$ is the division polynomial for $E[3]$.

Proof. We prove the statement for F_i; the other two are similar. Note that $(x - x_R)$ is the monic polynomial with divisor $(R) + (-R) - 2(\mathcal{O})$ where $\mathcal{O}$ is the identity point,

for all $R = (x_R, y_R) \in E$. Hence

$$D_i = (P) + (Q) + (2P) + (2Q) - (P+Q) - (2P+Q) - (2P+2Q) - (P+2Q)$$

is the divisor of $f_i = \dfrac{(x - x_P)(x - x_Q)}{(x - x_{P+Q})(x - x_{2P+Q})}$. Therefore $F_i = f_i + \frac{1}{f_i}$ is as claimed, where we note that ψ_3 is by definition the monic quartic polynomial with roots x_P, x_Q, x_{P+Q}, x_{2P+Q}. □

Now let $\mathfrak{p}$ be a prime of $\mathcal{K}$ such that $\mathfrak{p} \nmid 3\Delta_E$ and the Frobenius automorphism $\phi : x \mapsto x^{\mathrm{Norm}_{\mathcal{K}/\mathbb{Q}}\mathfrak{p}}$ has order 4 on the residue field of $\mathcal{K}(E[3])$ at any prime $\mathfrak{P}$ above $\mathfrak{p}$.

Let $\tilde{P}, \tilde{Q} \in \tilde{E}[3]$ be points of order 3 such that $\tilde{Q} \neq \phi^r(\tilde{P})$ for any r, so that they are necessarily a basis. Construct the principal Weil divisor

$$(\tilde{P}) + (\phi(\tilde{P})) + (\phi^2(\tilde{P})) + (\phi^3(\tilde{P})) - (\tilde{Q}) - (\phi(\tilde{Q})) - (\phi^2(\tilde{Q})) - (\phi^3(\tilde{Q}))$$

and let $g \in \dfrac{\mathcal{O}_{\mathcal{K}(E[3])}}{\mathfrak{P}}(\tilde{E})^\times$ be the corresponding monic function. As before, we then define $G = g + \frac{1}{g} \in \dfrac{\mathcal{O}_{\mathcal{K}}}{\mathfrak{p}}(\tilde{E})^\times$.

Theorem 6.3.10. *Let $E/\mathcal{K}$ be an elliptic curve over a number field $\mathcal{K}$ and suppose that $\mathrm{Im}\,\rho_{E,3} \cong Q_8$. Fix a basis P, Q of $E[3]$ and let $i = \left(\begin{smallmatrix} 0 & 2 \\ 1 & 0 \end{smallmatrix}\right), j = \left(\begin{smallmatrix} 2 & 2 \\ 2 & 1 \end{smallmatrix}\right), k = ij \in \mathrm{Aut}(E[3])$ with respect to this basis. Let $\mathfrak{p}$ be a prime of $\mathcal{K}$ such that $\mathfrak{p} \nmid 3\Delta_E$ and $\rho_{E,3}(\mathrm{Frob}_\mathfrak{p})$ is $\mathrm{GL}_2(\mathbb{F}_3)$-conjugate to i.*

Suppose F_i, F_j, F_k (constructed as above) are distinct modulo $\mathfrak{p}$. Then

i. $\rho_{E,3}(\mathrm{Frob}_\mathfrak{p})$ is $\mathrm{Gal}(\mathcal{K}(E[3])/\mathcal{K})$-conjugate to i if and only if $F_i \equiv G \mod \mathfrak{p}$;

ii. $\rho_{E,3}(\mathrm{Frob}_\mathfrak{p})$ is $\mathrm{Gal}(\mathcal{K}(E[3])/\mathcal{K})$-conjugate to j if and only if $F_j \equiv G \mod \mathfrak{p}$;

iii. $\rho_{E,3}(\mathrm{Frob}_\mathfrak{p})$ is $\mathrm{Gal}(\mathcal{K}(E[3])/\mathcal{K})$-conjugate to k if and only if $F_k \equiv G \mod \mathfrak{p}$.

Proof. First note that since $\rho_{E,3}(\mathrm{Frob}_\mathfrak{p})$ is $\mathrm{GL}_2(\mathbb{F}_3)$-conjugate to i, it is $\mathrm{Gal}(\mathcal{K}(E[3])/\mathcal{K})$-conjugate to one of i, j, k so suppose this is also i (with respect to a global basis P, Q), without loss of generality. To construct G, one can use the reduced basis $\tilde{P}, \tilde{Q}$ under which the Frobenius automorphism acts as $\pm i$, where $i^2 = -\mathrm{Id}$. Since the divisor is invariant under the action $R \mapsto -R$, we have $F_i \equiv G \mod \mathfrak{p}$. The converse follows since we have imposed that F_i, F_j, F_k are distinct $\mathrm{mod}\mathfrak{p}$. □

Example 6.3.11. *Consider $E/\mathcal{K} : y^2 = x^3 + x + 1$ where $\mathcal{K} = \mathbb{Q}(\zeta_3, \Delta_E^{1/3})$. This has a surjective mod 3 representation over $\mathbb{Q}$, so $\mathrm{Gal}(\mathbb{Q}(E[3])/\mathcal{K}) \cong Q_8$. We perform our*

computations over $\mathbb{C}$ so choose an embedding $\mathcal{K} \hookrightarrow \mathbb{C}$ by letting $\zeta_3 = \dfrac{-1+i\sqrt{3}}{2}$ and $\Delta_E^{1/3}$ to be the real cube root.

Let $P \approx (0.080, -1.040), Q \approx (0.571 - 1.754i, 0.496 + 1.940i)$ be a basis for $E[3]$. Then by computing the remaining torsion points and using Lemma 6.3.9, we find

$$\begin{aligned} F_i &\approx \frac{2x^4 - (6.61 + 9.14i)x^2 - 8x + (-4.13 + 2.98i)}{x^4 + 2x^2 + 4x - \frac{1}{3}}; \\ F_j &\approx \frac{2x^4 + 9.22x^2 - 8x + 11.59}{x^4 + 2x^2 + 4x - \frac{1}{3}}; \\ F_k &\approx \frac{2x^4 - (6.61 - 9.14i)x^2 - 8x + (-4.13 - 2.98i)}{x^4 + 2x^2 + 4x - \frac{1}{3}}. \end{aligned}$$

Now consider the prime $\mathfrak{p} = (11, 1 + \Delta_E^{1/3})$ of $\mathcal{K}$. We compute that $\tilde{E}(\mathbb{F}_{11^2}) = 140$ and hence the trace of Frobenius is zero mod 3 and the image is conjugate to one of i, j, k. Moreover, we find that $G = \dfrac{2x^4 + 3x + 9}{x^4 + 2x^2 + 4x + 7} \in \dfrac{\mathcal{O}_\mathcal{K}}{\mathfrak{p}}(\tilde{E})$.

To determine which one G is congruent to, we need to interpret our rational functions in $\mathcal{K}(E)$. One can show[3] that $F_j = \dfrac{2x^4 + \frac{4}{3}(-\Delta_E^{1/3} - 1)x^2 - 8x + \frac{1}{9}(\Delta_E^{2/3} - 4\Delta_E^{1/3} + 10)}{x^4 - 2x^2 - \frac{1}{3}}$. Moreover one can compute that since i, j, k are $\mathrm{GL}_2(\mathbb{F}_3) \cong \mathrm{Gal}(\mathbb{Q}(E[3])/\mathbb{Q})$ conjugate, F_i, F_k correspond to the other choices of a cube root of the discriminant.

Now we can check their reductions $\bmod \mathfrak{p}$ and we find $\rho_{E,3}(\mathrm{Frob}_\mathfrak{p})$ is $\mathrm{Gal}(\mathcal{K}(E[3])/\mathcal{K})$-conjugate to j.

For our second example, we consider an elliptic curve over $\mathbb{Q}$ whose mod 3 image is not surjective since its discriminant is already a rational cube. In this case, the image is equal to the normaliser of the nonsplit Cartan subgroup but this breaks the conjugacy of F_i, F_j and F_k as we shall see.

Example 6.3.12. *Consider $E/\mathbb{Q}(\zeta_3) : y^2 = x^3 - x$ which has discriminant $\Delta_E = 64 = 4^3$ and whose mod 3 image is isomorphic to Q_8. Once again we embed $\mathbb{Q}(\zeta_3) \hookrightarrow \mathbb{C}$ via $\zeta_3 = \dfrac{-1+i\sqrt{3}}{2}$ and choose a basis $P \approx (1.468, -1.302), Q \approx (-1.468, -1.302i)$ for $E[3]$.*

[3] We actually do this algebraically using Proposition 6.3.16, but one can also use the Lenstra–Lenstra–Lovász algorithm [LLL82] instead with the Minkowski embedding of $\mathcal{K}$.

With these choices, we find:

$$\begin{aligned} F_i &\approx \frac{2x^4 - 4x^2 + 4.67}{x^4 - 2x^2 - \frac{1}{3}}; \\ F_j &\approx \frac{2x^4 + (4 - 4.62i)x^2 - 0.67}{x^4 - 2x^2 - \frac{1}{3}}; \\ F_k &\approx \frac{2x^4 + (4 + 4.62i)x^2 - 0.67}{x^4 - 2x^2 - \frac{1}{3}}, \end{aligned}$$

from which we determine that

$$\begin{aligned} F_i &= \frac{2x^4 - 4x^2 + \frac{14}{3}}{x^4 - 2x^2 - \frac{1}{3}}; \\ F_j &= \frac{2x^4 + \frac{1}{3}(4 - 16\zeta_3)x^2 - \frac{2}{3}}{x^4 - 2x^2 - \frac{1}{3}}; \\ F_k &= \frac{2x^4 + \frac{1}{3}(4 + 16\zeta_3^2)x^2 - \frac{2}{3}}{x^4 - 2x^2 - \frac{1}{3}}. \end{aligned}$$

Now let $\mathfrak{p} = (5)$ be a prime of $\mathbb{Z}[\zeta_3]$. Computing the number of points of $\tilde{E}(\mathbb{F}_{25})$, we again find that the trace is zero mod 3 and hence the Frobenius element has order 4. In this case, we find $G = \dfrac{2x^4 + x^2 + 3}{x^4 + 3x^2 + 3}$ and F_i, F_j, F_k are distinct mod 5 so we may apply our results and find that $\rho_{E,3}(\mathrm{Frob}_{\mathfrak{p}})$ is $\mathrm{Gal}(\mathbb{Q}(E[3])/\mathbb{Q}(\zeta_3))$-conjugate to i.

Remark 6.3.13. *Here F_j and F_k are $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugate, whereas F_i is "fake- conjugate"; they each correspond to choosing a cube root of Δ_E so the fake-conjugate arises from the real cube root which happens to be rational. In fact, we can compute that the quadratic term is $\frac{1}{3}(-4\Delta^{1/3}+4)$ and the constant term is $\frac{1}{9}(\Delta^{2/3}+4\Delta^{1/3}+10)$.*

Remark 6.3.14. *We could have exploited this fake-conjugacy further by observing that since 5 was inert in $\mathbb{Q}(\zeta_3)$, the corresponding Frobenius element couldn't be j or k as our prime is stable under the Galois action. We elaborate more on this below.*

Corollary 6.3.15. *Let $E/\mathbb{Q}(\zeta_3)$ be the base change of an elliptic curve $E'/\mathbb{Q}$ such that $\mathrm{Im}\,\rho_{E,3} \cong Q_8$ and $\Delta_{E'} \in (\mathbb{Q}^\times)^3$. Let p be a rational prime, $\mathfrak{p} = p\mathbb{Z}[\zeta_3]$. Fix a basis P, Q for $E[3]$ and suppose, without loss of generality, that $F_i \in \mathbb{Q}(E)$ is the unique choice which may be defined over $\mathbb{Q}$. Suppose the following conditions hold:*

i. $p \equiv 2 \mod 3$*;*

ii. $p \nmid \Delta_{E'}$*;*

iii. $|\tilde{E}(\mathbb{F}_{p^2})| \equiv 2 \mod 3$*;*

iv. the functions F_i, F_j, F_k are distinct $\bmod \mathfrak{p}$.

Then $\rho_{E,3}(\mathrm{Frob}_\mathfrak{p})$ is $\mathrm{Gal}(\mathbb{Q}(E[3])/\mathbb{Q}(\zeta_3))$-conjugate to i.

Conversely, if $p \equiv 1 \mod 3$ and $\mathfrak{p}$ is any prime of $\mathbb{Z}[\zeta_3]$ above p which doesn't divide $\Delta_{E'}$, then $\rho_{E,3}(\mathrm{Frob}_\mathfrak{p})$ is not *$\mathrm{Gal}(\mathbb{Q}(E[3])/\mathbb{Q}(\zeta_3))$-conjugate to i.*

Proof. All but the first condition are the standard assumptions so that the image of Frobenius has order 4; the first one ensures that p is inert in $\mathbb{Z}[\zeta_3]$ and hence $\mathfrak{p}$ is stable under the action of $\mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q})$. For the converse, p splits so $\mathfrak{p}$ is not Galois invariant. □

Finally, we give a general form for the rational functions F_i, F_j, F_k; this enables us to do our calculations over $\mathbb{C}$ much easier.

Proposition 6.3.16. *Let $E/\mathcal{K} : y^2 = x^3 + Ax + B$ be an elliptic curve over a number field. Then the functions F_i, F_j, F_k have the form*

$$\frac{2x^4 - \frac{4}{3}(A + \Delta_E^{1/3})x^2 - 8Bx + \frac{1}{9}(\Delta_E^{2/3} - 4A\Delta_E^{1/3} + 10A^2)}{x^4 + 2Ax^2 + 4Bx - \frac{1}{3}A^2},$$

for some choice of the cube root of the discriminant $\Delta_E^{1/3}$.

Proof. Let $\psi_3 = x^4 + 2Ax^2 + 4Bx - \frac{1}{3}A^2$, the division polynomial for $E[3]$, have roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ and let $F \in \{F_i, F_j, F_k\}$.

Then $F\psi_3 = (x - \alpha_1)^2(x - \alpha_2)^2 + (x - \alpha_3)^2(x - \alpha_4)^2$ for some ordering of the α_i by Lemma 6.3.9. Expanding this, we find $F\psi_3 = 2x^4 + \left(-2\sum_i \alpha_i\right)x^3 + \left(4(\alpha_1\alpha_2 + \alpha_3\alpha_4) + \sum_i \alpha_i^2\right)x^2 - 2(\alpha_1\alpha_2^2 + \alpha_1^2\alpha_2 + \alpha_3\alpha_4^2 + \alpha_3^2\alpha_4)x + (\alpha_1^2\alpha_2^2 + \alpha_3^2\alpha_4^2)$.

Using ψ_3, we find:

$$\begin{aligned}
\sum_m \alpha_m &= 0; \\
\sum_m \alpha_m^2 &= \left(\sum_m \alpha_m\right)^2 - 2\sum_{m \neq n} \alpha_m\alpha_n = -4A; \\
\alpha_1\alpha_2^2 + \alpha_1^2\alpha_2 + \alpha_3\alpha_4^2 + \alpha_3^2\alpha_4 &= \prod_m \alpha_m \left(\sum_m \alpha_m\right) - \sum_{m,n,r \text{ distinct}} \alpha_m\alpha_n\alpha_r = 4B.
\end{aligned}$$

Let $\delta = \alpha_1\alpha_2 + \alpha_3\alpha_4$. Then $\alpha_1^2\alpha_2^2 + \alpha_3^2\alpha_4^2 = \delta^2 - 2\prod_m \alpha_m = \delta^2 - \frac{2}{9}A^4$ and we have

$F\psi_3 = 2x^4 + (4\delta - 4A)x^2 - 8Bx + (\delta^2 + \frac{2}{3}A^2)$.

Now recall from the proof of Lemma 6.3.3 that δ is a root of the resolvent cubic and hence $\delta = \frac{2}{3}A - \frac{1}{3}\Delta_E^{1/3}$ for some choice $\Delta_E^{1/3}$ of the cube root of the discriminant. Substituting this back in completes the proof. □

Appendix A

Table of lawful genus two hyperelliptic curves

Recall that an abelian variety $A/\mathcal{K}$ is said to be lawful if $W(A/\mathcal{F}) = 1$ for every quadratic extension $\mathcal{F}/\mathcal{K}$, equivalently every quadratic twist of A has the same root number. Moreover, we say $A/\mathcal{K}$ is lawful good (respectively lawful evil) if $W(A/\mathcal{K})$ is positive (respectively negative). Furthermore, the parity conjecture implies that if $A/\mathcal{K}$ is lawful evil, then all of its quadratic twists have odd rank and hence contain infinitely many rational points.

Below we give a table of lawful genus two hyperelliptic curves (by which we mean that their Jacobians are lawful), ordered by conductor up to $50,000$. The list of curves used as our input data was obtained from [BSS$^+$16, Col17]. As root numbers are invariant under isogeny, we only list curves with non-isogenous Jacobians. Note that the model given in the table is not necessarily minimal.

We do not claim completeness of the table for conductor at most $50,000$; indeed the original source is not necessarily complete and moreover we are unable to compute root numbers in cases of wild ramification so only checked curves with conductor coprime to $30 = 2 \times 3 \times 5$. All our curves will have the form $C : y^2 = f(x)$ so we only give the polynomial f in the table below.

$f(x)$	Conductor	Lawful good/ evil
$x^6+4x^5+6x^4+2x^3+x^2+2x+1$	169	Good
$x^6-4x^5+2x^4+2x^3+x^2+2x+1$	529	Good
$x^6+2x^5+7x^4+6x^3+13x^2+4x+8$	841	Good
$x^6+4x^5+6x^4+6x^3+x^2-2x-3$	961	Good
$x^6-2x^4+6x^3+13x^2+6x+1$	3721	Good
$x^6+4x^5+2x^4+2x^3+x^2-2x+1$	4489	Good
$-3x^6+4x^5-2x^4+2x^3+x^2-2x+1$	4489	Evil
$-3x^6+2x^5+29x^4-6x^3-82x^2+4x+73$	4489	Good
$x^6+2x^5+x^4+6x^3+2x^2-4x+1$	5329	Good
$-3x^6-32x^5-62x^4+102x^3-159x^2+126x-31$	5329	Good
$4x^5+5x^4+6x^3-3x^2-8x-4$	5929	Good
$x^6-12x^5+38x^4-26x^3-7x^2+6x+1$	8281	Good
$4x^5+33x^4+46x^3+13x^2-4x$	8281	Good
$x^6+2x^5+9x^4+10x^3+26x^2+12x+25$	9409	Good
$x^6+2x^4+2x^3+5x^2+6x+1$	10609	Good
$x^6-10x^4+2x^3+21x^2-18x+5$	10609	Evil
$x^6+2x^5+5x^4+2x^3-2x^2-4x-3$	11449	Good
$4x^5-11x^4+2x^3+9x^2-4x$	11881	Good
$-3x^6-4x^5+30x^4+30x^3-111x^2-50x+137$	17689	Good
$4x^5-15x^4+10x^3+5x^2-4x$	17689	Good
$x^6-10x^4-10x^3+5x^2+6x+1$	17689	Good
$x^6+8x^5+10x^4+6x^3+5x^2+2x+1$	17689	Good
$x^6+2x^5+9x^4+2x^3-6x^2-28x+21$	17689	Good
$4x^5+17x^4+14x^3-3x^2-4x$	24649	Good
$x^6+4x^5+2x^4+2x^3-3x^2-2x-3$	27889	Good
$x^6-8x^4-8x^3+8x^2+12x-8$	28561	Evil
$x^6+4x^5+2x^4+2x^3+41x^2+78x+41$	32761	Good
$x^6+2x^4+2x^3+5x^2-6x+1$	36481	Good
$x^6+2x^4-14x^3+5x^2+6x+1$	37249	Good
$x^6+2x^5+3x^4+4x^3+7x^2+14x+13$	43681	Good
$-3x^6+2x^5+21x^4-18x^3-30x^2+16x+17$	44521	Good
$x^6+4x^5+2x^4+6x^3+x^2-2x+1$	48841	Good
$-3x^6+8x^5-18x^4+26x^3-23x^2+10x-3$	48841	Good
$x^6+4x^5-4x^4-22x^3+8x^2+8x-71$	49729	Good

Remark A.0.17. *Note that for conductors* 4489 *and* 10609*, we get examples of both good and evil lawful Jacobians; in the former case the lawful good Jacobians also have distinct analytic ranks.*

On the other hand, we have only lawful good Jacobians for conductors $5329, 8281, 17689$ *and* 48841*. Moreover, every isogeny class of Jacobians of conductor* $5329, 17689$ *and* 48841 *listed in [BSS*$^+$*16, Col17] is lawful.*

Remark A.0.18. *We have found numerous examples above of lawful abelian varieties over* $\mathbb{Q}$*; this does not happen with elliptic curves over* $\mathbb{Q}$ *(or indeed any odd-dimensional abelian variety) by Lemma 4.4.4.*

Bibliography

[AD17] S. Anni and V. Dokchitser, *Constructing hyperelliptic curves with surjective Galois representations*, arXiv: 1701.05915 (2017).

[Art23] E. Artin, *Über die zetafunktionen gewisser algebraischer Zahlkörper*, Math. Annalen **89** (1923), 147–156.

[BCDT01] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over Q: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939.

[BCP97] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265.

[BDD16] S. Bettin, C. David, and C. Delauney, *Families of elliptic curves with non-zero average root number*, arXiv: 1612.03095 (2016).

[Bis18] M. Bisatt, *Frobenius elements in Galois representations with SL_n image*, Journal of Number Theory (to appear) **188** (2018), 165–171.

[BKS18] A. Brumer, K. Kramer, and M. Sabitova, *Explicit determination of root numbers of abelian varieties*, Trans. Amer. Math. Soc. **370** (2018), 2589–2604.

[BSD63] B. Birch and H. Swinnerton-Dyer, *Notes on elliptic curves I*, Crelle **212** (1963), 7–25.

[BSD65] ———, *Notes on elliptic curves II*, Crelle **218** (1965), 79–108.

[BSS+16] A. Booker, J. Sijsling, A. Sutherland, J. Voight, and D. Yasaki, *A database of genus 2 curves over the rational numbers*, arXiv:1602.03715 (2016).

[Buh78] J. Buhler, *Icosahedral Galois representations*, vol. 654, Springer-Verlag, 1978.

[Cas91] J. Cassels, *Lectures on elliptic curves*, Cambridge University Press, London Math. Soc. Student Texts 24, 1991.

[Col17] LMFDB Collaboration, *The L-functions and modular forms database*, http://www.lmfdb.org (2017).

[CW77] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. (1977), no. 39, 223–251.

[DD09a] T. Dokchitser and V. Dokchitser, *Elliptic curves with all quadratic twists of positive rank*, Acta Arithmetica **137** (2009), 193–197.

[DD09b] ———, *Self-duality of Selmer groups*, Math. Proc. Cambridge Philos. Soc. **146** (2009), 257–267.

[DD10] ———, *On the Birch–Swinnerton-Dyer quotient modulo squares*, Ann. Math. **172** (2010), no. 1, 567–596.

[DD11] ———, *Root numbers and parity of ranks of elliptic curves*, Crelle **2011** (2011), no. 658, 39–64.

[DD13] ———, *Identifying Frobenius elements in Galois groups*, Algebra and Number Theory **7** (2013), no. 6, 1325–1352.

[DDMM] T. Dokchitser, V. Dokchitser, C. Maistret, and A. Morgan, *Arithmetic of hyperelliptic curves over local fields*, In preparation.

[DDR16] L. Dembélé, F. Diamond, and D. Roberts, *Serre weights and wild ramification in two-dimensional Galois representations*, Forum of Mathematics, Sigma **4** (2016).

[Del73] P. Deligne, *Formes modulaires et représentations de GL(2)*, Modular functions of one variable II, Springer-Verlag, 1973, pp. 55—-105.

[Del79] ———, *Valeurs de fonctions L et périodes d'intégrales*, Automorphic Forms, Representations and L-Functions, Proc. Symp. Pure Math Vol 33 - Part 2, Amer. Math. Soc., 1979, pp. 313–346.

[Des16] J. Desjardins, *On the variation of the root number in families of elliptic curves*, arXiv: 1610.07440 (2016).

[DT02] W. Duke and A. Tóth, *The splitting of primes in division fields of elliptic curves*, Experimental Mathematics **11** (2002), no. 4, 555–565.

[FLS15] N. Freitas, B. Le Hung, and S. Siksek, *Elliptic curves over real quadratic fields are modular*, Invent. Math. **201** (2015), 159–206.

[FQ73] A. Fröhlich and J. Queyrut, *On the functional equation of the Artin L-function for characters of real representations.*, Invent. Math. **20** (1973), 125–138.

[Gal65] P. Gallagher, *Determinants of representations of finite groups*, Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg **28** (1965), no. 3-4, 162–167.

[Gow75] R. Gow, *Schur indices and modular representations*, Math. Z. **144** (1975), no. 2, 97–99.

[Gro72] A. Grothendieck, *Modèles de Néron et monodromie*, Groupes de Monodromie en Géométrie Algébrique, SGA7 I, Lecture Notes in Mathematics 288, Springer, 1972, pp. 313–523.

[GZ86] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320.

[Hel04] H. Helfgott, *On the behaviour of root numbers in families of elliptic curves*, arXiv: 0408141 (2004).

[Isa76] I. Isaacs, *Character theory of finite groups*, Academic Press Inc., 1976.

[Kol88] V. Kolyvagin, *Finiteness of E(Q) and sha(E/Q) for a subclass of Weil curves*, Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), no. 3, 522–540.

[LLL82] A. Lenstra, H. Lenstra, and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Annalen **261** (1982), no. 4, 515–534.

[Mas13] N. Mascot, *Computing modular Galois representations*, Rendiconti del Circolo Matematico di Palermo **62** (2013), no. 3, 451–476.

[Mil72] J. Milne, *On the arithmetic of abelian varieties*, Invent. Math. **17** (1972), 177–190.

[Mor15] A. Morgan, *2-Selmer parity for hyperelliptic curves in quadratic extensions*, arXiv: 1504.01960 (2015).

[MR10] B. Mazur and K. Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem*, Invent. Math. **181** (2010), no. 3, 541–575.

[Olt09] G. Olteanu, *Computation and applications of Schur indices*, Proceedings of the International Conference on Modules and Representation Theory, Cluj University Press, 2009, pp. 149–157.

[PRS11] C. Popescu, K. Rubin, and A. Silverberg, *Arithmetic of L-functions*, vol. 18, American Mathematical Society, 2011.

[Rob04] D. Roberts, *Frobenius classes in alternating groups*, Rocky Mountain J. Math **34** (2004), no. 4, 1483–1496.

[Roh90] D. Rohrlich, *The vanishing of certain Rankin-Selberg convolutions*, Automorphic Forms and Analytic Number Theory, Univ. Montréal, Montréal, QC, 1990, pp. 123–133.

[Roh94] ———, *Elliptic curves and the Weil–Deligne group*, Elliptic Curves and Related Topics, CRM Proc. & Lect. Notes, Vol. 4, American Mathematical Society, 1994, pp. 125–157.

[Roh96] ———, *Galois theory, elliptic curves, and root numbers*, Compositio Mathematica **100** (1996), no. 3, 311–349.

[Sab07] M. Sabitova, *Root numbers of abelian varieties*, Trans. Amer. Math. Soc. **359** (2007), 4259–4284.

[Sab13] ———, *Twisted root numbers and ranks of abelian varieties*, Journal of Combinatorics and Number Theory **V** (2013), no. 5, 25–30.

[Sch85] R. Schoof, *Elliptic curves over finite fields and the computation of square roots mod p*, Mathematics of Computation **44** (1985), no. 170, 483–494.

[Sch95] ———, *Counting points on elliptic curves over finite fields*, Journal de Théorie des Nombres de Bordeaux **7** (1995), no. 1, 219–254.

[Ser77] J. Serre, *Linear representations of finite groups*, Springer Science & Business Media, 1977.

[Sil13] J. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Springer Science & Business Media, 2013.

[ST68] J. Serre and J. Tate, *Good reduction of abelian varieties*, The Annals of Mathematics **88** (1968), no. 3, 492–517.

[Sto95] M. Stoll, *Two simple 2-dimensional abelian varieties defined over Q with Mordell-Weil group of rank at least 19*, C. R. Acad. Sci. Paris, Série I **321** (1995), no. 10, 1341–1345.

[Sut16] A. Sutherland, *Computing images of Galois representations attached to elliptic curves*, Forum of Mathematics, Sigma **4** (2016), e4.

[Tat66] J. Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki **9** (1966), no. 306, 415–440.

[Tat79] ———, *Number theoretic background*, Automorphic Forms, Representations and L-Functions, Proc. Symp. Pure Math Vol 33 - Part 2, American Mathematical Society, 1979, pp. 3–26.

[TW95] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. Math. **141** (1995), no. 3, 553–572.

[VA11] A. Várilly-Alvarado, *Density of rational points on isotrivial rational surfaces*, Algebra and Number Theory **5** (2011), no. 5, 659–690.

[vB17] R. van Bommel, *Numerical verification of the Birch and Swinnerton-Dyer conjecture for hyperelliptic curves of higher genus over Q up to squares*, arXiv:1711.10409 (2017).

[Wil95] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. Math. **141** (1995), no. 3, 443–551.

[YZ15] L. Yin and J. Zeng, *On the computation of coefficients of modular forms: the reduction modulo p approach*, Mathematics of Computation **84** (2015).

[Zen14] J. Zeng, *Computing Galois representations of modular abelian surfaces*, LMS Journal of Computation and Mathematics **17** (2014), no. A, 36–48.